8-2007

ESTIMATES RELATED TO THE ARITHMETIC OF ELLIPTIC CURVES

Bryan Faulkner
Clemson University, blfaulk@clemson.edu

ESTIMATES RELATED TO THE ARITHMETIC OF ELLIPTIC CURVES

A Dissertation
Presented to
the Graduate School of
Clemson University

In Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy
Mathematical Sciences

---

by
Bryan Faulkner
August 2007

Accepted by:
Dr. Kevin James, Committee Chair
Dr. Neil Calkin
Dr. Hiren Maharaj
Dr. Gretchen Matthews

ABSTRACT

This dissertation presents results related to two problems in the arithmetic of elliptic curves.

Let $E_n : y^2 = x^3 - n^2x$ denote the family of congruent number elliptic curves. In [13], Feng and Xiong equate the nontriviality of the Selmer groups associated with E_n to the presence of certain types of partitions of graphs associated with the prime factorization of n. The triviality of the Selmer groups associated to E_n implies that E_n has rank zero which in turn implies n is noncongruent. In chapter 2 (see [12]), we extend the ideas of Feng and Xiong in order to compute the Selmer groups of E_n.

Let E be an elliptic curve defined over some Abelian number field K with ring of integers $\mathcal{O}_K$. For a prime $\mathfrak{p}$ of degree f in $\mathcal{O}_K$ let $a_{\mathfrak{p}}(E)$ be the trace of the Frobenius morphism. Let p be a rational prime such that $\mathfrak{p}$ lies above p. By Hasse's theorem, we know that $a_{\mathfrak{p}}(E)$ satisfies the inequality $|a_{\mathfrak{p}}(E)| \leq 2p^{f/2}$. For a fixed integer r we define

$$\pi_E^{r,f}(x) = \#\{\mathfrak{p} \ : \ N(\mathfrak{p}) \leq x, \, deg_K(\mathfrak{p}) = f, \text{ and } a_{\mathfrak{p}}(E) = r\}.$$

A generalization of the Lang-Trotter conjecture for elliptic curves over number fields asserts that there exists a positive real constant $C_{E,r,f}$ such that

$$\pi_E^{r,f}(x) \sim C_{E,r,f} \begin{cases} \frac{\sqrt{x}}{\log x}, & \text{if } f = 1 \\ \log\log x, & \text{if } f = 2 \\ 1, & \text{otherwise.} \end{cases}$$

In chapter 3 we prove an average version of the above conjecture. For the $f = 1$ and $f = 2$ cases we calculate an explicit constant.

TABLE OF CONTENTS

CHAPTER 1

Introduction

We begin with an overview of some basic facts in the theory of elliptic curves. For more details we refer the reader to [32] and [33].

Let K be a field. An *elliptic curve* E with coefficients in K is a *smooth* cubic curve containing at least one K-rational point. The elliptic curve E may be realized as the set of solutions to the following *Weierstrass* equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

where $a_1, a_2, a_3, a_4, a_6 \in K$. If the characteristic of K is not 2 or 3, then we may write

$$E : y^2 = x^3 + ax + b$$

where a and b belong to K. We define $E(K)$ to be the set

$$E(K) := \{(x, y) \in K \times K : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$$

where $\mathcal{O}$ is the point on E at infinity. The condition that E be smooth is equivalent to requiring that the cubic $x^3 + ax + b$ have no multiple roots. This holds if and only if the discriminant of E is non-zero.

Definition 1.0.1. *The discriminant of the elliptic curve E denoted Δ_E is defined by*

$$\Delta_E := -16(4a^3 + 27b^2).$$

1.0.1 The Group Law

Consider $K = \mathbb{Q}$, where $\mathbb{Q}$ is the field of rational numbers. Let E be the elliptic curve given by

$$E : y^2 = x^3 + Ax + B$$

where A and B belong to K. We say that E is *defined* over K whenever $A, B \in K$. Consider the set of *rational points* on E,

$$E(\mathbb{Q}) = \{(x, y) \in \mathbb{Q}^2 : y^2 = x^3 + Ax + B; x, y \in \mathbb{Q}\} \cup \{\mathcal{O}\}.$$

Suppose P and Q are *distinct* rational points on E. Let l be the line containing P and Q. (Note that l has rational coefficients.) If l intersects E at a third point *different* from P and Q, then this third point denoted $P * Q$ is a rational point on E. If l is tangent to E at P [resp. Q], then $P * Q := P$ [resp. $P * Q := Q$]. Since, if a cubic polynomial with rational coefficients has two rational roots, then it has three rational roots counting multiplicity.

We define $P + Q$ to be the reflection of $P * Q$ about the x-axis. Suppose P and Q are *not* distinct. That is, suppose $P = Q$, then we take l to be the tangent line to the the elliptic curve at P. If the line l intersects E at a rational point different from P, then we denote this rational point by $P * P$. If no such point exists, then we must work in the projective plane. We give a brief description of the projective plane with an example which applies to this scenario.

Let K be a field. The *affine plane* (or *Euclidean plane*) with coordinates in K is defined to be the set

$$\{(x, y) : x, y \in K\}.$$

We denote the affine plane by $\mathbb{A}^2(K)$. An *affine curve* is a curve defined by a polynomial in two variables.

Example 1.0.2. *The elliptic curve E_0 defined by*

$$E_0 : y^2 = x^3 - x$$

is an affine curve. The elliptic curve E_0 is defined by the polynomial $g(x, y) = y^2 - x^3 + x$. Note that $(\pm 1, 0)$ and $(0, 0)$ are rational points on E_0, since $y^2 = x(x-1)(x+1)$. Let P denote the point $(1, 0)$. The line tangent to $g(x, y) = 0$ at P is given by

$$l_0 : x = 1.$$

In the affine plane $l_0 \cap E_0 = P$. Therefore, $P * P$ does not lie on the affine curve E_0. That is, the curves $y^2 = x^3 - x$ and $x = 1$ intersect at only one point in the affine plane. Therefore, in order to find $P * P$ we need to add points to the affine plane. These additional points are called the points at infinity.

To that end, we define the *projective plane* with coordinates in K to be the set of triples (a, b, c), with a, b, and c not all zero, such that two triples (a, b, c) and (a', b', c') are considered to be the same point if there is a nonzero λ such that $a = \lambda a'$, $b = \lambda b'$, and $c = \lambda c'$. Note that this defines an equilvalence relation on K^3. The numbers a, b, and c are called the *homogeneous coordinates* for the point (a, b, c). We denote the projective plane by $\mathbb{P}^2(K)$.

A *homogeneous polynomial of degree d* is a polynomial $F(X, Y, Z)$ which satisfies the identity

$$F(\lambda X, \lambda Y, \lambda Z) = \lambda^d F(X, Y, Z).$$

A *projective curve* (or *algebraic curve*) in the projective plane is defined to be the set of solutions to an equation

$$C : F(X, Y, Z) = 0$$

where $F(X, Y, Z)$ is a non-constant homogeneous polynomial. The *degree of the projective curve* C is the degree of the polynomial F.

Example 1.0.3. *Consider the homogeneous polynomial*

$$G(X, Y, Z) = ZY^2 - X^3 + XZ^2$$

of degree 3. *The set of solutions to* $G(X, Y, Z) = 0$ *defines a projective curve*

$$C : G(X, Y, Z) = 0.$$

If we define a (non-homogeneous) polynomial

$$f(x, y) := F(x, y, 1),$$

then we get a bijection

$$\begin{aligned} \{(a, b, c) \in C : c \neq 0\} &\longrightarrow \{(x, y) \in \mathbb{A}^2 : f(x, y) = 0\} \\ (a, b, c) &\mapsto \left(\frac{a}{c}, \frac{b}{c}\right). \end{aligned}$$

We call the affine curve $f(x, y) = 0$ the *affine part* of the projective curve C.

Example 1.0.4. *Let* C *be the projective curve given in Example 1.0.3. Then the affine part of* C *is defined by the polynomial*

$$g(x, y) := G(x, y, 1) = y^2 - x^3 + x.$$

The points (a, b, c) on C with $c = 0$ are called the *points at infinity*. So, we wish to view elliptic curves as projective curves. The process of replacing a homogeneous polynomial $F(X, Y, Z)$ by a non-homogeneous polynomial $f(x, y) = F(x, y, 1)$ is called *dehomogenization*. We can *homogenize* a polynomial $f(x, y)$ by multiplying each term by an appropriate power of z.

More precisely, the *homogenization* of $f(x, y)$ is

$$F(x, y, z) = z^d f\left(\frac{x}{z}, \frac{y}{z}\right)$$

where d is the degree of f. In this way we are able to write elliptic curves as projective curves.

Example 1.0.5. *The homogenization of* $y^2 = x^3 - x$ *is* $y^2z = x^3 - xz^2$. *Define the projective curve*

$$E : y^2z = x^3 - xz^2.$$

We make the following observations.

1. *The equation* $y^2 = x^3 - x$ *gives an elliptic curve defined over* $\mathbb{Q}$, *which is the affine curve in Example 1.0.2, denoted* E_0.
2. E_0 *is the affine part of* E.

Recall $(1, 0)$ *is a rational point on* E_0 *and* $x = 1$ *is tangent to* E_0 *at* $(1, 0)$. *The homogenization of* $x = 1$ *is* $x = z$ *which defines the line*

$$l : x = z$$

in $\mathbb{P}^2$. *Substituting* $x = z$ *into the homogenization of* E_0 *yields*

$$zy^2 = z^3 - z^3$$

$$\Leftrightarrow zy^2 = 0.$$

Clearly, $zy^2 = 0$ *has two solutions,* $y = 0$ *and* $z = 0$. *Therefore,*

$$E \cap l = \{(1, 0, 1), (1, 0, 0)\}.$$

We denote this additional point of intersection by $\mathcal{O}$.

Let K be a field with characteristic different from 2 or 3. Recall that elliptic curves defined over K have Weiestrass equations

$$y^2 = x^3 + ax + b.$$

The homogenization of this equation yields

$$y^2z = x^3 + axz^2 + bz^3.$$

Where does this cubic equation intersect the line at infinity $z = 0$? Substituting $z = 0$ into the equation gives $x^3 = 0$. So, the elliptic curve intersects the line at infinity at one point, the point at infinity.

Given two rational points P and Q on an elliptic curve E and a line l containing P and Q. We have provided evidence that there exists a third point $P * Q$ on $E \cap l$ as long as we work over the projective plane. Define the addition of P and Q, denoted $P + Q$ to be the reflection of $P * Q$ about the x-axis. We can derive an explicit addition formula for points on elliptic curves as follows. Let E be an elliptic curve given by

$$E : y^2 = x^3 + Ax + B$$

where $A, B \in \mathbb{Q}$. Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be distinct points on E such that $x_1 \neq x_2$. Let $P * Q = (x_3, -y_3)$, then $P + Q = (x_3, y_3)$. An equation for the line containing P and Q is given by

$$l : y = M(x - x_1) + y_1$$

where $M = \frac{y_1 - y_2}{x_1 - x_2}$. Since, $(x_3, -y_3) \in l \cap E$, the y-coordinate of $P + Q$ is given by $y_3 = M(x_1 - x_3) - y_1$. To find x_3 in terms of x_1 and x_2 observe

$$\begin{aligned} y_3^2 = x_3^3 + Ax_3 + B &\Rightarrow (M(x_3 - x_1) + y_1)^2 = x_3^3 + Ax_3 + B \\ &\Rightarrow x_3^3 + Ax_3 + B - [M(x_3 - x_1) + y_1]^2 = 0. \end{aligned}$$

Let $p(x) = x^3 + Ax + B - [M(x - x_1) + y_1]^2$. Zeros of $p(x)$ are the x-coordinates of the points in $E \cap l$. Therefore, we have

$$x^3 + Ax + B - [M(x - x_1) + y_1]^2 = (x - x_1)(x - x_2)(x - x_3). \tag{1.1}$$

Equating coefficients of x^2 on each side of (1.1) gives

$$\begin{aligned} M^2 &= x_1 + x_2 + x_3 \\ \Rightarrow x_3 &= M^2 - x_1 - x_2. \end{aligned} \tag{1.2}$$

Thus,

$$\begin{aligned} x_3 &= \left(\frac{y_1 - y_2}{x_1 - x_2}\right)^2 - x_1 - x_2 \\ y_3 &= \left(\frac{y_1 - y_2}{x_1 - x_2}\right)(x_1 - x_3) - y_1 \\ &= \left(\frac{y_1 - y_2}{x_1 - x_2}\right)(x_1 - \left(\frac{y_1 - y_2}{x_1 - x_2}\right)^2 + x_1 + x_2) - y_1. \end{aligned}$$

There are two other cases to consider. If $x_1 = x_2$, then $P = \pm Q$ and $P + Q = \mathcal{O}$. If $P = Q$, then recall from above that we look at the tangent line to E at P to get $2P$ ($2P$ is interpreted as $P + P$). Using implicit differentiation we find the slope M of this

tangent line to be $M = \frac{3x_1^2+A}{2y_1}$. By the same arguments as above we have

$$x_3 = \left(\frac{3x_1^2 + A}{2y_1}\right)^2 - x_1 - x_1$$

and

$$y_3 = \left(\frac{3x_1^2 + A}{2y_1}\right)\left(x_1 - \left(\frac{3x_1^2 + A}{2y_1}\right) + x_1 + x_1\right) - y_1. \tag{1.3}$$

The above process works over any field with characteristic not equal to 2 or 3. In particular, let $\mathbb{F}_p$ be the field containing p elements. We can reduce the addition formulas given by (1.2) and (1.3) modulo p, for any prime p exceeding 3. Thus, we have an addition law for points on elliptic curves over $\mathbb{F}_p$. Recall that we define $E(\mathbb{Q})$ to be the set

$$E(\mathbb{Q}) := \{(x, y) \in \mathbb{Q} \times \mathbb{Q} : y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\}.$$

We list the following three facts without proof (see [32, Chapter 3 Proposition 2.2]). For the operation '+' defined above we have

1. for any $P, Q, R \in E(\mathbb{Q})$, $P + (Q + R) = (P + Q) + R$,
2. for any $P \in E(\mathbb{Q})$, $P + \mathcal{O} = \mathcal{O} + P = \mathcal{O}$, and
3. if $P = (x, y)$, then $P + (-P) = \mathcal{O}$, where $-P = (x, -y)$.

Thus, $E(\mathbb{Q})$ equipped with $+$ is a group. By the discussion above it is clear that for any $P, Q \in E(\mathbb{Q})$ we have $P + Q = Q + P$. Therefore, $E(\mathbb{Q})$ is an Abelian group. In [28] Mordell proved that $E(\mathbb{Q})$ is finitely generated. That is, one may write

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \times E(\mathbb{Q})_{tor}$$

where $E(\mathbb{Q})_{tor}$ is the subgroup of torsion elements of $E(\mathbb{Q})$. Weil [36] generalized Mordell's result to any number field and Abelian varieties of any dimension (see [5]). In [32] Mazur completely characterized $E(\mathbb{Q})_{tor}$ by proving

Theorem 1.0.6. *(Mazur)*

$$E(\mathbb{Q})_{tor} \cong \begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{where } n = 0, 1, 2, \ldots 10, 12 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}, & \text{where } n = 1, 2, 3, 4. \end{cases}$$

While there are algorithms to compute the torsion subgroup of $E(\mathbb{Q})$ (see [10]), no general algorithm is known to compute r, which we call the rank of the curve. However, Selmer groups give an upper bound on the rank of E. We discuss Selmer groups in section 1.1.

1.0.2 Elliptic Curves Over Finite Fields

Let $E_{a,b}$ be an elliptic curve defined over $\mathbb{F}_p$ with Weiestrass equation

$$E_{a,b} : y^2 = x^3 + ax + b.$$

The elliptic curves $E_{a',b'}$ over $\mathbb{F}_p$ which are $\mathbb{F}_p$-*isomorphic* to $E_{a,b}$ are given by all choices

$$a' = u^4 a \text{ and } b' = u^6 b$$

with $u \in \mathbb{F}_p^*$. Let $p \in \mathbb{Z}$ be a prime greater than 3. The equation above is called a *minimal model for* $E_{a,b}$ *at* p if $\text{ord}_p(\Delta_{E_{a,b}})$ is minimized subject to the condition that $a, b \in \mathbb{Z}$. [32, pg. 172] gives the following

Fact 1.0.7. *With the notation above: Let* p *be a prime greater than* 3*.*

The equation is minimal at p *if and only if* $a, b \in \mathbb{Z}$ *and* $\text{ord}_p(\Delta_{E_{a,b}}) < 12$*.*

We wish to study $E_{a,b}$ over finite fields. To that end, we *reduce the curve modulo* p as follows. Given an elliptic curve $E_{a,b}$ defined over $\mathbb{F}_p$, we select a minimal model E_{au^4,bu^6} for $E_{a,b}$ and define

$$E^p_{\bar{a},\bar{b}} : y^2 = x^3 + \overline{au^4}x + \overline{u^6 b}$$

where $\overline{au^4}$ and $\overline{u^6b}$ are the residues modulo p of au^4 and bu^6 respectively. The elliptic curve $E^p_{\overline{a},\overline{b}}$ is called the *reduction of $E_{a,b}$ modulo p*. We note that $E^p_{\overline{a},\overline{b}}$ may be singular (nonsmooth). But, since we started with a minimal equation for $E_{a,b}$, the equation for $E^p_{\overline{a},\overline{b}}$ is unique up to the standard change of coordinates

$$x = u^2x' \qquad y = u^3y' \qquad \text{for } u \in \mathbb{F}_p^*.$$

If $E^p_{\overline{a},\overline{b}}$ is nonsingular, then we say that $E_{a,b}$ has *good reduction modulo p*. On the other hand, if $E^p_{\overline{a},\overline{b}}$ is singular, then we say that $E_{a,b}$ has *bad reduction modulo p*.

Fact 1.0.8. *([32, Chapter 7 Proposition 5.1]) The elliptic curve $E_{a,b}$ has good reduction modulo p if and only if* $\mathrm{ord}_p(\Delta_{E_{a,b}}) = 0$.

Let $\mathbb{F}_q$ be the finite field with q elements, where q is a prime power. Let E be an elliptic curve defined over $\mathbb{F}_q$, then $E(\mathbb{F}_q)$ is a finite Abelian group (see [32, Chapter 3 §2]). One might ask about the size of $E(\mathbb{F}_q)$. It turns out that the size of $E(\mathbb{F}_q)$ is always near $q+1$. Hasse proved the following result which had been conjectured by Artin (see [32, Chapter 5]).

Theorem 1.0.9. *(Hasse's Theorem) Let E be an elliptic curve defined over $\mathbb{F}_q$, and let $\#E(\mathbb{F}_q)$ be the number of $(x,y) \in \mathbb{F}_q \times \mathbb{F}_q$ which satisfy E along with $\mathcal{O}$. Then*

$$|\#E(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}.$$

The error in approximating $\#E(\mathbb{F}_q)$ by $q+1$ plays an important role in the arithmetic of elliptic curves. So, we make the following definition.

Definition 1.0.10. *For an elliptic curve E defined over $\mathbb{F}_p$ define $a_E(p)$ as*

$$a_E(p) := p + 1 - \#E(\mathbb{F}_p).$$

We call $a_E(p)$ the *trace of the Frobenius morphism* for reasons which we will explain later. Note that by Hasse's Theorem $|a_E(p)| \leq 2\sqrt{p}$.

1.0.3 The Endomorphism Ring of an Elliptic Curve

Let E_1 and E_2 be elliptic curves. An *isogeny* between E_1 and E_2 is a homomorphism $\phi : E_1 \to E_2$ defined by rational functions.

Example 1.0.11. *Let E be an elliptic curve. For $m \in \mathbb{Z}$, the multiplication by m isogeny $[m] : E \to E$ is defined by*

$$[m](P) := \begin{cases} \underbrace{P + P + \cdots P}_{m \text{ times}} & \text{if } m > 0 \\ \mathcal{O} & \text{if } m = 0 \\ \underbrace{(-P) + (-P) + \cdots + (-P)}_{|m| \text{ times}} & \text{if } m < 0. \end{cases}$$

For an elliptic curve E we define

$$\mathrm{End}(E) := \{\text{isogenies } \phi : E \to E\}.$$

The set, $\mathrm{End}(E)$ is called the *ring of endomorphisms* of E. For ϕ_1 and ϕ_2 belonging to $\mathrm{End}(E)$ we define addition in $\mathrm{End}(E)$ by $(\phi_1+\phi_2)(P) = \phi_1(P)+\phi_2(P)$ and multiplication is defined by $(\phi_1\phi_2)(P) = \phi_1(\phi_2(P))$. Usually $\mathrm{End}(E) \cong \mathbb{Z}$, but whenever there are endomorphisms other than the multiplication by m isogenies we say that E has *complex multiplication*. If E is defined over a finite field, then $\mathrm{End}(E)$ is always larger than $\mathbb{Z}$ (see [32, Chapter 5 Theorem 3.1]).

Example 1.0.12. *Suppose E is defined over $\mathbb{F}_p$, where p is prime. The Frobenius endomorphism $\phi_{\mathrm{Frob}} : E \to E$ is defined by $\phi(x, y) = (x^p, y^p)$.*

The *degree* of an isogeny ϕ is $\#\ker(\phi)$, denoted by $\deg(\phi)$. The proof in [32, Chapter 5] of Hasse's Theorem requires the fact that the set of points fixed by ϕ_{Frob} is exactly

$E(\mathbb{F}_p)$. Observe for $P \in E(\mathbb{F}_p)$,

$$\begin{aligned}(1 - \phi_{\text{Frob}})(P) &= [1](P) + [-1](\phi_{\text{Frob}}(P)) \\ &= P - P \\ &= \mathcal{O}.\end{aligned}$$

Suppose $Q \in \ker(1 - \phi_{\text{Frob}})$. Then

$$\begin{aligned}&(1 - \phi_{\text{Frob}})(Q) = \mathcal{O} \\ &\Rightarrow [1](Q) + [-1](\phi_{\text{Frob}}(Q)) = Q - Q \\ &\Rightarrow [-1](\phi_{\text{Frob}}) = -Q \\ &\Rightarrow Q \in E(\mathbb{F}_p).\end{aligned}$$

Thus, $E(\mathbb{F}_p) = \ker(1 - \phi_{\text{Frob}})$. So,

$$\#E(\mathbb{F}_p) = \#\ker(1 - \phi_{\text{Frob}}) = \deg(1 - \phi_{\text{Frob}}).$$

Let E_1 and E_2 be elliptic curves. For an isogeny $\phi : E_1 \to E_2$ there exists a *dual isogeny* $\phi' : E_2 \to E_1$ such that $\phi' \circ \phi = [m] \in \text{End}(E_1)$ and $\phi \circ \phi' = [m] \in \text{End}(E_2)$ where $m = \deg(\phi)$. From the structure of $\text{End}(E_1)$ ϕ satisfies the degree 2 polynomial

$$(X - \phi)(X - \phi') = X^2 - (\phi + \phi')X + \phi \circ \phi' \in \mathbb{Z}[X]$$

(see [32, Chapter 5]). Therefore, we define the *trace of an isogeny* ϕ to be the isogeny $\phi + \phi'$. We denote the trace of an isogeny ϕ by $\text{tr}(\phi)$.

Fact 1.0.13. *With the notation above*

$$\begin{aligned}\#E(\mathbb{F}_p) &= \deg(1 - \phi\text{Frob}) \\ &= 1 - a + p\end{aligned}$$

where $[a] = \text{tr}(\phi_{\text{Frob}})$. *([32, Chapter 5 Theorem 4.1(a)]).*

1.0.4 Torsion Points

An element P of any group under addition (with identity $\mathcal{O}$) is said to have order m whenever m is the smallest positive integer such that

$$\underbrace{P + P + \cdots P}_{m \text{ times}} = \mathcal{O}.$$

If no such m exists, then P is said to have infinite order. The notation mP should be interpreted as

$$\underbrace{P + P + \cdots P}_{m \text{ times}}.$$

Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve defined over a field K. Let $\overline{K}$ be an algebraic closure of K (e.g. $K = \mathbb{Q}$ and $\overline{K} = \mathbb{C}$). Let $E[n]$ denote the set of points of order dividing n from $E(\overline{K})$. That is,

$$E[n] = \{P \in E(\overline{K}) : nP = \mathcal{O}\}.$$

If $P \in E[2]$, then

$$\begin{aligned} & 2P = \mathcal{O} \\ \Rightarrow \quad & P = -P \\ \Rightarrow \quad & \text{the } y\text{-coordinate of } P \text{ is } 0. \end{aligned}$$

So, $E[2] = \{\mathcal{O}\} \cup \{(0, x) | 0 = x^3 + Ax + B\}$. Therefore, $\#E[2] = 4$. Since $E[2]$ has no point of order 4, $E[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Also,

$$\begin{aligned} P \in E[3] \Rightarrow 3P &= \mathcal{O} \\ \Rightarrow 2P &= -P. \end{aligned}$$

So, if $P = (x, y)$, then using the formulas for $2P$ given by (1.3), we have

$$\begin{aligned} &x\text{-coor. of } -P = x\text{-coor. of } 2P \\ &\Rightarrow x = \left(\frac{3x^2 + A}{2y}\right)^2 - 2x \\ &\Rightarrow 12xy^2 = 9x^4 + 6Ax^2 + A^2. \end{aligned}$$

Substituting $y^2 = x^3 + Ax + B$ we have $3x^4 + 6Ax^2 + 12xB - A^2 = 0$. Let $q(x) = 3x^4 + 6Ax^2 + 12xB - A^2$. The polynomial, q is called the 3-division polynomial (see [32, pg. 105 exercise 3.7]). It turns out that since E is smooth, q has no multiple roots. Each root of q is the x-coordinate of a point $P \in E[3]$. Therefore, $E[3] = \{\mathcal{O}\} \cup \{(r_i, \pm\sqrt{r_i^3 + Ar_i + B}) : i = 1, 2, 3, 4\}$ where the r_i are the roots of q. We see that $\#E[3] = 9$ and since each point has order 1 or 3, $E[3] \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Fact 1.0.14. *If E is defined over $\mathbb{Q}$, then*

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

(see [32, Chapter 3 Corollary 6.4]).

1.0.5 Galois Representations

Let E be an elliptic curve defined over $\mathbb{Q}$ and $m \geq 2$. Let $K = \mathbb{Q}(E[m])$ and let $\mathcal{O}_K$ denote the ring of integers of K. The Galois group $\mathrm{Gal}(K/\mathbb{Q})$ acts on $E[m]$. So, we consider the Galois representation

$$\rho_{E,m} : \mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{Aut}(E[m]).$$

Since $\mathrm{Aut}(E[m]) \cong \mathrm{Aut}(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}) = \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$, we may fix a basis for $E[m]$ and identify $\mathrm{Aut}(E[m])$ with $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. Thus the action of $\mathrm{Gal}(K/\mathbb{Q})$ on $E[m]$ induces a representation

$$\rho_{E,m} : \mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}).$$

Let $\mathfrak{p} \in \mathcal{O}_K$ be a prime ideal which lies above the prime $p \in Z$. Let $\sigma_p \in \mathrm{Gal}(K/\mathbb{Q})$ be the Frobenius element above p (i.e. $\sigma_p(x) \equiv x^p \pmod{\mathfrak{p}}$ for all $x \in \mathcal{O}_K$). It can be shown that

$$\mathrm{tr}[\rho_{E,m}(\sigma_p)] \equiv a_E(p) \pmod{m}$$

where for $A \in \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$, $\mathrm{tr}(A)$ denotes the trace of A (see [32, Chapter 3 §7 and Chapter 5 §2]).

1.1 Selmer Groups

In this section we introduce some basic facts on Selmer groups of an elliptic curve. For details the reader is referred to [32, Chapter 10].

In order to define Selmer groups of elliptic curves we appeal to the following theorem (see [32, Chapter 10 Proposition 4.9]).

Theorem 1.1.1. *Let $E/\mathbb{Q}$ and $E'/\mathbb{Q}$ be elliptic curves given by the equations*

$$E : y^2 = x^3 + ax^2 + bx \quad \textit{and} \quad E' : Y^2 = X^3 - 2aX^2 + (a^2 - 4b)X;$$

and let the map $\phi : E \to E'$ defined by $\phi(x, y) = (y^2/x^2, y(b - x^2)/x^2)$ be the isogeny of degree 2 with kernel $E[\phi] = \{\mathcal{O}, (0, 0)\}$. Let $S = \{$primes dividing $2b(a^2 - 4b)\}$. Let C_d be the equation in variables w and z given by

$$C_d : dw^2 = d^2 - 2adz^2 + (a^2 - 4b)z^4.$$

and $\mathbb{Q}(S, 2) = \{d \in \mathbb{Q}^*/\mathbb{Q}^{*2} : \mathrm{ord}_p(d) \equiv 0 \pmod{2}$ for all $p \notin S\}$. The ϕ-Selmer group is then

$$S^{(\phi)} = \{d \in \mathbb{Q}(S, 2) : C_d(\mathbb{R}) \neq \emptyset; C_d(\mathbb{Q}_p) \neq \emptyset \textit{ for all } p \in S\}.$$

Note that the Selmer group is determined by local information. In particular, one must show the existence of p-adic solutions to the equations C_d for a *finite* set of primes. Then d belongs to the Selmer group provided that C_d possesses a real solution. For the

isogeny ϕ above there exists a *dual* isogeny $\phi' : E' \to E$ such that $\phi \circ \phi' = [2]$, where $[2]$ is the multiplication by 2 map on E (see [32, Chapter 3 Example 4.5]). We may apply Theorem 1.1.1 using the isogeny ϕ' in place of ϕ to obtain the ϕ'-Selmer group $S^{(\phi')}$. Since the Selmer groups are subgroups of $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ we may write

$$S^{(\phi)}(E/\mathbb{Q}) \cong \left(\mathbb{Z}/2\mathbb{Z}\right)^{s(\phi)}, \quad S^{(\phi')}(E/\mathbb{Q}) \cong \left(\mathbb{Z}/2\mathbb{Z}\right)^{s(\phi')},$$

for some nonnegative integers $s(\phi)$ and $s(\phi')$. Recall that $E(\mathbb{Q})$ is finitely generated. So, we may write

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \times E(\mathbb{Q})_{tor}.$$

If E has at least one rational point of order 2 (which is required for our definition of the Selmer groups), then

$$r \leq s(\phi) + s(\phi') - 2$$

(see [16]). In chapter 2 we explicitly compute Selmer groups associated with the curve $E_n : y^2 = x^3 - n^2x$.

1.2 The Trace of the Frobenius Morphism and the Distribution of Prime Numbers

Dirichlet's theorem on primes in arithmetic progressions asserts that for coprime integers a and b there are infinitely many primes which are congruent to a modulo b. Moreover, Dirichlet's theorem says

$$\pi(x; a, b) := \#\{p \leq x : p \text{ is prime } ;\ p \equiv a \pmod{b}\} \sim \frac{1}{\phi(b)}\pi(x)$$

where ϕ is the Euler totient function and $\pi(x) = \#\{p \leq x : p \text{ is prime}\}$.
In the search for an analogous result Hardy and Littlewood in [17] explored primes in quadratic progressions and made the following

Conjecture 1.2.1. *Let $q(n) = an^2+bn+c$ be a quadratic progression with $gcd(a, b, c) = 1$ and $b^2 - 4ac \neq t^2$ for any $t \in \mathbb{Z}$. Let*

$$\pi(x; q) = \#\{p \leq x : p = q(n) \text{ for some } n\}.$$

Then

$$\pi(x; q) \sim C\pi_{1/2}(x)$$

where $\pi_{1/2}(x) = \int_2^x \frac{\mathrm{dt}}{2\sqrt{t}\log t} \sim \frac{\sqrt{x}}{\log x}$ and C is a constant.

Let E be an elliptic curve defined over the rationals and let p be an odd prime. Denote the field containing p elements by $\mathbb{F}_p$. If E has good reduction modulo p, then we consider E defined over $\mathbb{F}_p$. Let $a_p(E)$ be the trace of the Frobenius morphism of E. Recall that $\#E(\mathbb{F}_p) = p + 1 - a_p(E)$ and $|a_p(E)| \leq 2\sqrt{p}$. Fix $r \in \mathbb{Z}$. It can be shown that if $r \neq 0$ and E has complex multiplication, the primes with a fixed trace of the Frobenius morphism are primes in quadratic progressions. In [26] Lang and Trotter proposed

Conjecture 1.2.2. *Define*

$$\pi_E^r(x) = \#\{p \leq x : a_p(E) = r\}.$$

Except for the case where $r = 0$ and E has complex multiplication, there is a constant $C_{E,r}$ depending only on E and r such that

$$\pi_E^r(x) \sim C_{E,r}\frac{\sqrt{x}}{\log x}.$$

Using probabilistic methods, Lang and Trotter predicted the constant $C_{E,r}$. More precisely, consider the Galois representation

$$\rho_{E,m} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}).$$

Let $G(m)$ denote the image of $\rho_{E,m}$, and let $G(m)_r$ denote the set of elements in $G(m)$ having trace r modulo m.

If E does not have complex multiplication, then the image of the Galois representation on the full torsion subgroup $E(\overline{\mathbb{Q}})_{tor}$ is an open subgroup of $\mathrm{GL}_2(\hat{\mathbb{Z}})$, where $\hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$ (see [31]). It follows that there exists an integer m_E such that $\rho_{E,l}$ is surjective for all primes l not dividing m_E and such that the image in $\mathrm{GL}_2(\hat{\mathbb{Z}})$ of the Galois representation on $E(\overline{\mathbb{Q}})_{tor}$ is the full inverse image of $G(m_E)$. The Lang-Trotter constant $C_{E,r}$ is then defined as [26, pg. 36]

$$\begin{aligned} C_{E,r} &= \frac{2}{\pi}\frac{m_E|G(M_E)_r|}{|G(m_E)|}\prod_{l\nmid m_E}\frac{l|G(l)_r|}{|G(l)|} \\ &= \frac{2}{\pi}\frac{m_E|G(m_E)_r|}{G(m_E)}\prod_{\substack{q\mid r \\ q\nmid m_E}}\frac{q^2}{q^2-1}\prod_{q\nmid r m_E}\frac{q(q^2-q-1)}{(q-1)^2(q+1)}. \end{aligned}$$

Let K be a number field of degree n over $\mathbb{Q}$. Let $\mathcal{O}_K$ denote the ring of integers of K. Fix $r \in \mathbb{Z}$, a positive integer f such that $f|n$, and an elliptic curve with good reduction modulo $\mathfrak{p}$. One may extend Lang and Trotter's conjecture to K by asking the following question. What can be said about the number of prime ideals with norm no greater than x, degree equal to f, and trace of the Frobenius morphism equal to r? The conjecture which offers an answer to this question can be stated as follows.

Conjecture 1.2.3. *There exists a constant $C_{E,r,f} \in \mathbb{R}^{\geq 0}$ such that*

$$\pi_E^{r,f}(x) \sim C_{E,r,f}\begin{cases} \frac{\sqrt{x}}{\log x}, & \text{if } f = 1 \\ \log\log x, & \text{if } f = 2 \\ 1, & \text{otherwise} \end{cases}$$

The constant $C_{E,r,f}$ can be 0, and the asymptotic relation is then interpretated to mean that there are only finitely many such primes.

In [8] David and Pappalardi obtained average results for $K = \mathbb{Q}(i)$ and $f = 2$ which are consistent with Conjecture 1.2.3 over number fields. In chapter 3 we consider K, any Abelian extension of $\mathbb{Q}$ and obtain average results for r odd and any $f|n$. One could obtain results similar to ours for even r with a bit more work.

CHAPTER 2

A Graphical Approach to Computing Selmer Groups

Throughout this chapter n will represent a positive square free integer greater than one. We will denote by $E_n : y^2 = x^3 - n^2x$, the family of congruent number curves. If $n = p_1 \cdots p_s$, then let

$$M =< -1, 2, p_1, \ldots, p_s > \subseteq \mathbb{Q}^*/(\mathbb{Q}^*)^2$$

We define (see [13], [32, Ch. 10 §4] for more details) Selmer groups S_n and S'_n by

$$\begin{aligned} S_n &= \{d \in M \mid \ C_d(\mathbb{Q}_p) \neq \emptyset \ \forall p|2n, \ C_d(\mathbb{Q}_\infty) \neq \emptyset\}, \\ S'_n &= \{d \in M \mid \ C'_d(\mathbb{Q}_p) \neq \emptyset \ \forall p|2n, \ C'_d(\mathbb{Q}_\infty) \neq \emptyset\}, \end{aligned}$$

where the equations C_d and C'_d, in variables (w, t, z) are given by

$$C_d : \ dw^2 = t^4 + (2n/d)^2 z^4, \quad C'_d : \ dw^2 = t^4 - (n/d)^2 z^4.$$

We should note that $(0, 0, 0)$ is always a solution to $C_d(C'_d)$. So, when we write $C_d(\mathbb{Q}_p) \neq \emptyset$ ($C'_d(\mathbb{Q}_p) \neq \emptyset$), we mean there exists nontrivial solutions.

There has been much interest in understanding these groups (see [19, 20, 24, 37] and references therein). In fact, in [19] Heath-Brown gives a formula for the average size of the Selmer group related to the congruent number curve.

In a paper of Feng and Xiong [13], graph theory is used to describe conditions such that S_n and S'_n are trivial, which in turn implies that the rank of E_n is zero. In [4] probabilities relating to graphs found in [13] are used to determine how many square-free integers yield 2-Selmer groups of a given size.

In this chapter we use graph theoretic concepts similar to those introduced in [13] to compute S_n and S'_n.

In order to understand S_n and S'_n, we must determine for which $d \in M$ the equations C_d and C'_d have solutions over $\mathbb{Q}_p$ for all $p|2n$. For odd primes p, we search for solutions over $\mathbb{F}_p$ and then invoke Hensel's lemma to lift solutions in $\mathbb{F}_p$ to solutions in $\mathbb{Q}_p$. The application of Hensel's lemma in the 2-adic case is a bit more difficult. However, in all but one case, it is sufficient to consider C_d and C'_d modulo 2^3 as solutions here will lift to solutions in $\mathbb{Q}_2$.

Following Feng and Xiong we make the following definitions.

Definition 2.0.4. *Let $n = p_1 \cdots p_t \cdot q_1 \cdots q_l$ with $p_i \equiv 1 \pmod 4$ and $q_j \equiv 3 \pmod 4$ for $0 \leq i \leq t$ and $0 \leq j \leq l$. Define a graph, $G(n)$, by defining the vertex set to be $V(G(n)) = \{p_1, \ldots, p_t, q_1, \ldots q_l\}$ and the edge set as*

$$\begin{aligned} E(G(n)) &= \{\overline{p_i p_j} \ : \ \left(\frac{p_i}{p_j}\right) = -1 \text{ for } 1 \leq i \leq t \text{ and } 1 \leq j \leq t\} \\ &\cup \{\overline{p_i q_j} \ : \ \left(\frac{p_i}{q_j}\right) = -1 \text{ for } 1 \leq i \leq t \text{ and } 1 \leq j \leq l\} \end{aligned}$$

Definition 2.0.5. *Let $n = 2 \cdot p_1 \cdots p_t \cdot q_1 \cdots q_l$ with $p_i \equiv 1 \pmod 4$ and $q_j \equiv 3 \pmod 4$ for $0 \leq i \leq t$ and $0 \leq j \leq l$. Define a graph $\overline{G}(n)$ in the following way.*

$$\begin{aligned} V(\overline{G}(n)) &= \{2, p_1, \ldots p_t, q_1, \ldots q_l\} \\ E(\overline{G}(n)) &= \{\overline{p_i p_j} \mid \left(\frac{p_j}{p_i}\right) = -1 \quad 0 \leq i \neq j \leq t\} \\ &\cup \{\overline{p_i q_j} \mid \left(\frac{p_i}{q_j}\right) = -1 \quad 0 \leq i \leq t, 0 \leq j \leq l\} \\ &\cup \{\overline{p_i 2} \mid \left(\frac{2}{p_i}\right) = -1 \quad 0 \leq i \leq t\} \end{aligned}$$

A partition of a vertex set V is an ordered pair (V_1, V_2) such that $V_1 \cap V_2 = \emptyset$ and $V_1 \cup V_2 = V$. The trivial partitions are $(\emptyset, V)$ and $(V, \emptyset)$. For $p \in V_2$, by $\#\{p \to V_1\}$ we will mean the number of vertices in V_1 adjacent to p. We will be interested in the partitions of V which are even in the following sense.

Definition 2.0.6. *Let $G = (V, E)$ be a directed graph. A partition (V_1, V_2) of V is even provided that for any vertex, $p \in V_1$ (V_2), $\#\{p \to V_2\ (V_1)\}$ is even. In this case, we shall write $(V_1, V_2) \vdash_e V$ (read "(V_1, V_2) is an even partition of V").*

Notice that the trivial partitions are even. We will also be interested in partitions of V which are *quasi-even* in the following sense.

Definition 2.0.7. *A partition (V_1, V_2) of V is quasi-even provided that for any vertex, $p \in V_1$ (V_2)*

$$\#\{p \to V_2(V_1)\} \equiv \begin{cases} 0 \pmod 2, & \text{if } \left(\frac{2}{p}\right) = 1 \\ 1 \pmod 2, & \text{if } \left(\frac{2}{p}\right) = -1. \end{cases}$$

In this case, we shall write $(V_1, V_2) \vdash_{qe} V$.

In this chapter, we prove that the number of even and quasi-even partitions of $G(n)$ ($\overline{G}(n)$, if n is even) predict the size of the Selmer group S_n. We also prove that the number of even partitions of similiar graphs predict the size of the Selmer group, S'_n. It will be clear from our proofs that the even and quasi-even partitions of these graphs correspond in a natural way to elements of S_n and S'_n.

Theorem 2.0.8. *Let $p_1, \ldots, p_t, q_1, \ldots, q_l$ be the odd prime factors of n, where $p_i \equiv 1 \pmod 4$ for $0 \leq i \leq t$ and $q_j \equiv 3 \pmod 4$ for $0 \leq j \leq l$ (t,l not both zero).*

1. *If $n \equiv \pm 1 \pmod 8$ and $\exists\, p|n$, $p \equiv \pm 3 \pmod 8$, then*

$$\begin{aligned} |S_n| = \; & \# \; \{(V_1, V_2) \vdash_e V(G(n)) \mid q_j \notin V_1;\ 0 \leq j \leq l\} + \\ & \# \; \{(V_1, V_2) \vdash_{qe} V(G(n)) \mid q_j \notin V_1;\ 0 \leq j \leq l\} \end{aligned}$$

2. *If $n \equiv \pm 3 \pmod 8$, then*

$$|S_n| = \#\{(V_1, V_2) \vdash_e V(G(n)) \mid q_j \notin V_1;\ 0 \leq j \leq l\}$$

3. *If $p_i \equiv 1 \pmod 8$ for all $0 \leq i \leq t$ and $q_j \equiv 7 \pmod 8$ for all $0 \leq j \leq l$, then*

$$|S_n| = 2 \cdot \#\{(V_1, V_2) \vdash_e V(G(n)) \mid q_j \notin V_1;\ 0 \leq j \leq l\}$$

4. *If $n \equiv 0 \pmod 2$, then*

$$|S_n| = \#\{(V_1, V_2) \vdash_e V(\overline{G}(n)) \mid q_j \notin V_1;\ 0 \leq j \leq l\}$$

In order to compute S'_n, we require three additional tools.

Definition 2.0.9. *Let $n = p_1 \cdots p_t \cdot q_1 \cdots q_l \equiv \pm 3 \pmod 8$ with $p_i \equiv 1 \pmod 4$ and $q_j \equiv 3 \pmod 4$ for $0 \leq i \leq t$ and $0 \leq j \leq l$. Define a graph, $g(n)$, by defining the vertex set to be $V(g(n)) = \{p_1, \ldots p_t, q_1, \ldots q_l\}$ and the edge set as*

$$\begin{aligned} E(g(n)) \; = \; & \{\overline{p_i p_j} \; : \; \left(\frac{p_i}{p_j}\right) = -1 \text{ for } 1 \leq i \leq t \text{ and } 0 \leq j \leq t\} \\ \cup \; & \{\overrightarrow{p_i q_j} \; : \; \left(\frac{p_i}{q_j}\right) = -1 \text{ for } 0 \leq i \leq t \text{ and } 0 \leq j \leq l\} \end{aligned}$$

Definition 2.0.10. *Let* $n = p_1 \cdots p_t \cdot q_1 \cdots q_l \equiv \pm 1 \pmod 8$ *with* $p_i \equiv 1 \pmod 4$ *and* $q_j \equiv 3 \pmod 4$ *for* $0 \leq i \leq t$ *and* $0 \leq j \leq l$. *Define a graph,* $G(-n)$, *by defining the vertex set to be* $V(G(-n)) = \{-1, p_1, \ldots p_t, q_1, \ldots q_l\}$ *and the edge set as*

$$\begin{aligned} E(G(-n)) &= \{\overline{p_i p_j} \ : \ \left(\frac{p_i}{p_j}\right) = -1 \text{ for } 0 \leq i \leq t \text{ and } 0 \leq j \leq t\} \\ &\cup \ \{\overrightarrow{p_i q_j} : \ \left(\frac{p_i}{q_j}\right) = -1 \text{ for } 0 \leq i \leq t \text{ and } 0 \leq j \leq l\} \\ &\cup \ \{\overrightarrow{-1 r} : \ r \in V(G(-n)) \quad \text{and} \quad r \equiv \pm 3 \pmod 8\} \end{aligned}$$

Definition 2.0.11. *Let* $n = 2 \cdot p_1 \cdots p_t \cdot q_1 \cdots q_l$ *with* $p_i \equiv 1 \pmod 4$ *and* $q_j \equiv 3 \pmod 4$ *for* $0 \leq i \leq t$ *and* $0 \leq j \leq l$. *Define a graph* $G'(n)$ *in the following way.*

$$\begin{aligned} V(G'(n)) &= \{2, p_1, \ldots p_t, q_1, \ldots q_l\} \\ E(G'(n)) &= \{\overline{p_i p_j} \mid \left(\frac{p_j}{p_i}\right) = -1 \quad 0 \leq i \neq j \leq t\} \\ &\cup \ \{\overrightarrow{p_i q_j} \mid \left(\frac{p_i}{q_j}\right) = -1 \quad 0 \leq i \leq t, 0 \leq j \leq l\} \\ &\cup \ \{\overrightarrow{p_i 2} \mid \left(\frac{2}{p_i}\right) = -1 \quad 0 \leq i \leq t\} \end{aligned}$$

Then we have the following theorem.

Theorem 2.0.12. *Let* n *be a positive square free integer greater than one.*

1. *If* $n \equiv \pm 3 \pmod 8$, *then*
$$|S'_n| = 2 \cdot \#\{(V_1, V_2) \vdash_e g(n)\}$$
2. *If* $n \equiv \pm 1 \pmod 8$, *then*
$$|S'_n| = \#\{(V_1, V_2) \vdash_e G(-n)\}$$
3. *If* $n \equiv 0 \pmod 2$, *then*
$$|S'_n| = 2 \cdot \#\{(V_1, V_2) \vdash_e G'(n)\}$$

The organization of the rest of this chapter is as follows. In section 2.1, we state several lemmas which allow us to characterize for which d, C_d and C'_d have nontrivial solutions in $\mathbb{Q}_p$. In sections 2.2 and 2.3, we prove Theorems 2.0.8 and 2.0.12. In section 2.4 we review some concepts of graph theory related to counting even partitions and give corollaries of the two theorems which are more amenable to computation. Finally, in section 2.5 we give an example and a remark concerning the generators of these groups.

2.1 $C_d(\mathbb{Q}_p)$ and $C'_d(\mathbb{Q}_p)$

In this section we wish to characterize, in terms of n and d, when C_d and C'_d have solutions over $\mathbb{Q}_p$, for $p|2n$, and over $\mathbb{Q}_\infty$. We first recall the following lemmas from [13].

Lemma 2.1.1. *(Feng and Xiong [13, lemma 3.1]) Let p be an odd prime, n an odd positive square free integer with odd prime divisors $\{p_1, \ldots, p_s\}$, and $d \in M =< -1, 2, p_1, \ldots p_s > \subseteq \mathbb{Q}^*/(\mathbb{Q}^*)^2$.*

1. $C_d(\mathbb{Q}_\infty) = \emptyset \iff d < 0$
2. *For $p|d$,* $C_d(\mathbb{Q}_p) \neq \emptyset \iff \left(\frac{n/d}{p}\right) = 1$ *and* $\left(\frac{-1}{p}\right) = 1$.
3. *For $p|2n/d$,* $C_d(\mathbb{Q}_p) \neq \emptyset \iff \left(\frac{d}{p}\right) = 1$
4. $d \equiv 1 \pmod 4 \implies C_d(\mathbb{Q}_2) \neq \emptyset$
5. $n \equiv \pm 3 \pmod 8$ *and* $2|d \implies C_d(\mathbb{Q}_2) = \emptyset$
6. $n \equiv \pm 1 \pmod 8$ *and* $d = 2d'|2n$ *and* $d' \equiv 1 \pmod 4 \implies C_d(\mathbb{Q}_2) \neq \emptyset$

Lemma 2.1.2. *(Feng and Xiong [13, lemma 3.2]) Let p be an odd prime, n an odd positive square free integer with odd prime divisors $\{p_1, \dots p_s\}$, and $d \in M =< -1, 2, p_1, \dots p_s > \subseteq \mathbb{Q}^*/(\mathbb{Q}^*)^2$.*

1. *For $p|d$, $C'_d(\mathbb{Q}_p) \neq \emptyset \iff \left(\frac{-1}{p}\right) = -1$ or $\left(\frac{n/d}{p}\right) = 1$.*
2. *For $p|n/d$, $C'_d(\mathbb{Q}_p) \neq \emptyset \iff \left(\frac{-1}{p}\right) = -1$ or $\left(\frac{d}{p}\right) = 1$.*
3. *If $d \equiv 1 \pmod 2$, then $C'_d(\mathbb{Q}_2) \neq \emptyset \iff d \equiv \pm 1 \pmod 8$ or $n/d \equiv \pm 1 \pmod 8$*
4. *If $d \equiv 0 \pmod 2$ then $C'_d(\mathbb{Q}_2) = \emptyset$.*

We introduce two additional lemmas to handle the cases when n is even.

Lemma 2.1.3. *Let p be an odd prime, n an even positive square free integer with odd prime divisors $\{p_1, \dots p_s\}$, and $d \in M =< -1, 2, p_1, \dots p_s > \subseteq \mathbb{Q}^*/(\mathbb{Q}^*)^2$.*

1. *$C_d(\mathbb{Q}_\infty) = \emptyset \iff d < 0$.*
2. *$d \equiv 0 \pmod 2 \implies C_d(\mathbb{Q}_2) = \emptyset$*
3. *For $p|d$, $C_d(\mathbb{Q}_p) \neq \emptyset \iff \left(\frac{n/d}{p}\right) = 1$ and $\left(\frac{-1}{p}\right) = 1$.*
4. *For $p|n/d$, $C_d(\mathbb{Q}_p) \neq \emptyset \iff \left(\frac{d}{p}\right) = 1$.*
5. *$d \equiv 1 \pmod 8 \implies C_d(\mathbb{Q}_2) \neq \emptyset$*
6. *$d \equiv 5 \pmod 8 \implies C_d(\mathbb{Q}_2) = \emptyset$*

Proof.

For the proofs of (1) and (2) see [13, lemma 5.1].

(3) ($\Leftarrow$) See [13, lemma 3.1].

(3) ($\Rightarrow$) Suppose $(w, t, z) \in C_d(\mathbb{Q}_p)$. Since $p|d$ we have,

$$-1 \equiv (2n/d)^2 z^4 t^{-4} \pmod p$$

so that $\left(\frac{-1}{p}\right) = 1$. Let $\alpha \in \mathbb{F}_p$ be such that $\alpha^2 \equiv -1 \pmod{p}$.

Then we have

$$\begin{aligned} &\alpha^2 (2n/d)^{-2} \equiv \left(z^2/t^2\right)^2 \qquad (\text{mod } p) \\ &\Rightarrow 1 = \left(\frac{\pm\alpha (2n/d)^{-1}}{p}\right) = \left(\frac{\alpha (2n/d)^{-1}}{p}\right) \quad \text{since} \quad \left(\frac{-1}{p}\right) = 1 \end{aligned}$$

Consider two cases. First, suppose $p \equiv 1 \pmod{8}$. Then

$$\left(\frac{\alpha}{p}\right) = 1 \Rightarrow \left(\frac{2n/d}{p}\right) = 1 \Rightarrow \left(\frac{n/d}{p}\right) = 1$$

Second, suppose $p \equiv 5 \pmod{8}$. We must have $\left(\frac{\alpha}{p}\right) = -1$. Therefore, we have

$$\left(\frac{2}{p}\right) = -1, \quad \left(\frac{\alpha 2^{-1}}{p}\right) = 1$$

and

$$\left(\frac{\alpha (2n/d)^{-1}}{p}\right) = 1$$

which implies

$$\left(\frac{n/d}{p}\right) = 1$$

(4) ($\Rightarrow$) This is clear.

(4) ($\Leftarrow$) Suppose $\left(\frac{d}{p}\right) = 1$. Then there exists an $\alpha \in \mathbb{F}_p$ such that $\alpha^2 \equiv d \ (mod\ p)$. We have,

$$\begin{aligned} dw^2 \equiv t^4 \ (mod\ p) &\Leftrightarrow \alpha^2 w^2 \equiv t^4 \ (mod\ p) \\ &\Leftrightarrow (\alpha w)^2 \equiv t^4 \ (mod\ p) \end{aligned}$$

Hence, $(w_0, t_0, z_0) = (\alpha^{-1}, 1, 0) \in C_d(\mathbb{F}_p)$. Using Hensel's lemma we may lift this solution to a solution in $\mathbb{Q}_p$ (see the argument for (5) below for example).

(5) For $d \equiv 1 \pmod{8}$, let $(w_0, t_0, z_0) = (1, 1, 0)$. This is a solution to $C_d \pmod{8}$ and we may lift this solution using Hensel's lemma. More explicitly, consider a solution

(w_0, t_0, z_0) to $C_d (mod\ 2^k)$ for $k \geq 3$ with w_0 odd. This is also a solution to $C_d (mod\ 2^{k-1})$. Let

$$w_1 = w_0 + 2^{k-1}m$$

$$t_1 = t_0 + 2^{k-1}s$$

$$z_1 = z_0 + 2^{k-1}l$$

for some integers m, s, and l. Write, $t_0^4 + \left(\frac{2n}{d}\right)^2 z_0^4 - dw_0^2 = 2^k N$ for some integer N. Substituting, we have

$$(t_0 + 2^{k-1}s)^4 + \left(\frac{2n}{d}\right)^2 (z_0 + 2^{k-1}l)^4 - d(w_0 + 2^{k-1}m)^2 \equiv 0 \pmod{2^{k+1}}$$

$$\Leftrightarrow 2^k N - 2^k d w_0 m \equiv 0 \pmod{2^{k+1}}$$

$$\Leftrightarrow N \equiv w_0 m \pmod 2$$

$$\Leftrightarrow N \equiv M \pmod 2 \quad \text{(because } w_0 \text{ is odd.)}$$

Thus, $C_d(\mathbb{Q}_2) \neq \emptyset$.

(6) Suppose (w', t', z') is a solution to C_d over $\mathbb{Q}_2$. Then (w', t', z') is a solution to C_d (mod 8). This gives, $d(w')^2 \equiv (t')^4$ (mod 8). Therefore, $2|t'$ and $4|w'$. Thus, $(W = w'/4, T = t'/2, z')$ is a solution to

$$\overline{C_d} : dw^2 = t^4 + (m/d)^2 z^4$$

where $m = n/2$. Thus, if C_d has solutions in $\mathbb{Q}_2$ then so does $\overline{C_d}$. We claim that $\overline{C_d}$ has no nontrivial solutions. To see this assume that $(0,0,0) \neq (w_0, t_0, z_0) \in \overline{C_d}(\mathbb{Q}_2)$. Note that if w_0, t_0, z_0 are all even then $4|w_0$, so we may divide w_0 by 4 and t_0, z_0 by 2 and obtain a new solution to $\overline{C_d}$. Thus, we may assume that at least one of w_0, t_0, z_0 is odd. However, we note that all solutions to $\overline{C_d}$ (mod 8) have w, t, z all even. Thus, there are no solutions to $\overline{C_d}$ in $\mathbb{Q}_2$. Therefore, there are no solutions to C_d in $\mathbb{Q}_2$ when $d \equiv 5$ (mod 8).

□

Lemma 2.1.4. *Let p be an odd prime, n an even positive square free integer with odd prime divisors $\{p_1, \dots p_s\}$, and $d \in M =< -1, 2, p_1, \dots p_s > \subseteq \mathbb{Q}^*/(\mathbb{Q}^*)^2$.*

1. $d \equiv 1 \pmod 2 \implies C'_d(\mathbb{Q}_2) \neq \emptyset$
2. $d \equiv 0 \pmod 2 \implies C'_d(\mathbb{Q}_2) \neq \emptyset$
3. *For $p|d$, $C'_d(\mathbb{Q}_p) \neq \emptyset \iff \left(\frac{-1}{p}\right) = -1$ or $\left(\frac{n/d}{p}\right) = 1$*
4. *For $p|n/d$, $C'_d(\mathbb{Q}_p) \neq \emptyset \iff \left(\frac{-1}{p}\right) = -1$ or $\left(\frac{d}{p}\right) = 1$*

Proof.

For the proofs of (1),(3), and (4) see [13, lemma 5.2].

(2) If $(n/d)^2 \equiv 9 \pmod{16}$, let $(w_0, t_0, z_0) = (2, 1, 1)$. If $(n/d)^2 \equiv 1 \pmod{16}$, let $(w_0, t_0, z_0) = (4, 1, 1)$. These are solutions to $C'_d \pmod{16}$ and we may lift these solutions using Hensel's lemma. More explicitly, consider a solution (w_0, t_0, z_0) to $C'_d (mod\ 2^k)$ for $k \geq 4$ and with t_0 odd. (w_0, t_0, z_0) is also a solution to $C'_d (mod\ 2^{k-1})$. Let

$$w_1 = w_0 + 2^{k-1}m$$
$$t_1 = t_0 + 2^{k-2}s$$
$$z_1 = z_0 + 2^{k-1}l$$

for some integers m, s, and l. Write, $t_0^4 - \left(\frac{n}{d}\right)^2 z_0^4 - dw_0^2 = 2^k N$ for some integer N. Substituting, we have

$$(t_0 + 2^{k-2}s)^4 - \left(\frac{n}{d}\right)^2 (z_0 + 2^{k-1}l)^4 - d(w_0 + 2^{k-1}m)^2 \equiv 0 \pmod{2^{k+1}}$$
$$\Leftrightarrow 2^k N + 2^k t_0^3 s \equiv 0 \pmod{2^{k+1}}$$
$$\Leftrightarrow N \equiv t_0^3 s \pmod 2$$

Since t_0 is odd take $s \equiv N t_0^{-3} (mod\ 2)$. Thus, $C_d(\mathbb{Q}_2) \neq \emptyset$. □

2.2 Proof of Theorem 2.0.8

We first establish a correspondence between odd positive elements of S_n with even partitions of $G(n)$. We will take empty products to be 1.

Lemma 2.2.1. *Let $n = p_1 \cdots p_t \cdot q_1 \cdots q_l$ with $p_i \equiv 1 \pmod 4$ and $q_j \equiv 3 \pmod 4$ for $0 \leq i \leq t$ and $0 \leq j \leq l$ (t,l not both zero). For every even partition, (V_1, V_2) of $V(G(n))$ such that V_1 contains no prime factors which are 3 modulo 4 we have d in S_n, where*

$$d = \prod_{p \in V_1} p$$

Proof. Suppose (V_1, V_2) is an arbitrary nontrivial even partition of $V(G(n))$ with V_1 containing no prime factors which are 3 modulo 4. Let

$$V_1 = \{p_1, \ldots, p_s\} \text{ for some } s,\ 1 \leq s \leq t$$

then

$$V_2 = \{p_{s+1}, \ldots p_t, q_1, \ldots q_l\}$$

Consider $d = p_1 \cdots p_s$. Notice here that $\left(\frac{-1}{p_i}\right) = 1$, thus one of the conditions of Lemma 2.1.1 (2) is satisfied. For any $1 \leq i \leq s$, we have

$$\begin{aligned}\left(\frac{n/d}{p_i}\right) &= \prod_{r \in V_2} \left(\frac{r}{p_i}\right) \\ &= (1)^{\#\{r \in V_2 : \overline{p_i r} \notin E(G(n))\}} \times (-1)^{\#\{r \in V_2 : \overline{p_i r} \in E(G(n))\}} \\ &= 1 \quad \text{since} \quad (V_1, V_2) \quad \text{is even}\end{aligned}$$

Therefore, $C_d(\mathbb{Q}_{p_i}) \neq \emptyset$ for $1 \leq i \leq s$ by Lemma 2.1.1 (2). Also, for $r \in V_2$

$$\begin{aligned}\left(\frac{d}{r}\right) &= \prod_{i=1}^{s} \left(\frac{p_i}{r}\right) \\ &= (1)^{\#\{p \in V_1 : \overline{pr} \notin E(G(n))\}} \times (-1)^{\#\{p \in V_1 : \overline{pr} \in E(G(n))\}} \\ &= 1 \quad \text{since} \quad (V_1, V_2) \quad \text{is even}\end{aligned}$$

Therefore, $C_d(\mathbb{Q}_r) \neq \emptyset$ for $r \in V_2$ by Lemma 2.1.1 (3). There is a point on C_d over $\mathbb{Q}_2$ by Lemma 2.1.1 (4), since $d \equiv 1 \pmod 4$. Therefore, $d \in S_n$.

□

Remark 2.2.2. *Suppose n is squarefree, and $d|n$. If $q \equiv 3 \pmod 4$ and $q|d$ then by Lemma 2.1.1 (2) $d \notin S_n$. That is, a necessary condition for a number to be in S_n is that the number have no prime factors which are 3 modulo 4.*

The next lemma shows that for any odd element, d, of the Selmer group, S_n, there exists an even partition, (V_1, V_2) of $V(G(n))$, with V_1 corresponding to d as in Lemma 2.2.1.

Lemma 2.2.3. *Let n be as in Lemma 2.2.1. Suppose d is odd and $d \in S_n$, by the above remark and Lemma 2.1.1 we may assume $d = p_1 \cdots p_s \in S_n$ for some s, $1 \leq s \leq t$, then, letting $V_1 = \{p_1, \ldots p_s\}$ and $V_2 = \{p_{s+1}, \ldots p_t, q_1, \ldots q_l\}$, (V_1, V_2) is an even partition of $V(G(n))$.*

Proof. Suppose $d = p_1 \cdots p_s$ is a member of S_n. By definition,

$$C_d(\mathbb{Q}_p) \neq \emptyset \ \ \forall p|2n \text{ and } C_d(\mathbb{Q}_\infty) \neq \emptyset$$

From Lemma 2.1.1 (2), for $p|d$, $\left(\frac{n/d}{p}\right) = 1$. Therefore, for $1 \leq i \leq s$

$$\begin{aligned} 1 = \left(\frac{n/d}{p_i}\right) &= \prod_{r \in V_2} \left(\frac{r}{p_i}\right) \\ &= (1)^{\#\{r \in V_2 : \overline{p_i r} \notin E(G(n))\}} \times (-1)^{\#\{r \in V_2 : \overline{p_i r} \in E(G(n))\}} \\ &\Rightarrow \quad \#\{p_i \to V_2\} \quad \text{is even} \end{aligned}$$

Similarly, Lemma 2.1.1 (3) gives $\left(\frac{d}{r}\right) = 1$ for $r|2n/d$. So that, for $1 \leq i \leq s$ and $r \in V_2$,

$$\begin{aligned} 1 = \left(\frac{d}{r}\right) &= \prod_{i=1}^{s} \left(\frac{p_i}{r}\right) \\ &\Rightarrow \#\{r \to V_1\} \quad \text{is even} \end{aligned}$$

Thus, (V_1, V_2) is an even partition of $V(G(n))$.

□

Now, we will establish a correspondence between the even positive elements of S_n with quasi-even partitions of $G(n)$.

Lemma 2.2.4. *Let $n = p_1 \cdots p_t \cdot q_1 \cdots q_l \equiv \pm 1 \pmod 8$ with $p_i \equiv 1 \pmod 4$ and $q_j \equiv 3 \pmod 4$ for $0 \leq i \leq t$ and $0 \leq j \leq l$ (t,l not both zero). For every quasi-even partition, (V_1, V_2) of $V(G(n))$ such that V_1 contains no prime factors which are 3 modulo 4 we have $2d$ in S_n, where*

$$d = \prod_{p \in V_1} p$$

Proof. Suppose (V_1, V_2) is an arbitrary nontrivial quasi-even partition of $V(G(n))$ with V_1 containing no prime factors which are 3 modulo 4. Let

$$V_1 = \{p_1, \ldots, p_s\} \text{ for some s, } 1 \leq s \leq t$$

then

$$V_2 = \{p_{s+1}, \ldots p_t, q_1, \ldots q_l\}$$

Let $d = p_1 p_2 \cdots p_s$. Consider $2d$. Notice here that $\left(\frac{-1}{p_i}\right) = 1$, thus one of the conditions of Lemma 2.1.1 (2) is satisfied. Suppose $p_i \equiv 1 \pmod 8$. Then

$$\begin{aligned}\left(\frac{n/2d}{p_i}\right) &= \left(\frac{2}{p_i}\right) \prod_{r \in V_2} \left(\frac{r}{p_i}\right) \\ &= (1) \times (1)^{\#\{r \in V_2 : \overline{p_i r} \notin E(G(n))\}} \times (-1)^{\#\{r \in V_2 : \overline{p_i r} \in E(G(n))\}} \\ &= 1 \times 1 \times 1 \quad \text{since} \quad (V_1, V_2) \quad \text{is quasi-even}\end{aligned}$$

Suppose $p_i \equiv 5 \pmod 8$. Then

$$\begin{aligned}\left(\frac{n/2d}{p_i}\right) &= \left(\frac{2}{p_i}\right)\prod_{r\in V_2}\left(\frac{r}{p_i}\right)\\ &= (-1)\times(1)^{\#\{r\in V_2:\overline{p_i r}\notin E(G(n))\}}\times(-1)^{\#\{r\in V_2:\overline{p_i r}\in E(G(n))\}}\\ &= -1\times 1\times -1 = 1 \quad \text{since} \quad (V_1,V_2) \quad \text{is quasi-even}\end{aligned}$$

Therefore, $C_{2d}(\mathbb{Q}_{p_i}) \neq \emptyset$ for $1 \leq i \leq s$ by Lemma 2.1.1 (2). Also, for $r \in V_2$. If $r \equiv \pm 1 \pmod 8$, then

$$\begin{aligned}\left(\frac{2d}{r}\right) &= \left(\frac{2}{r}\right)\prod_{i=1}^{s}\left(\frac{p_i}{r}\right)\\ &= (1)\times(1)^{\#\{p\in V_1:\overline{pr}\notin E(G(n))\}}\times(-1)^{\#\{p\in V_1:\overline{pr}\in E(G(n))\}}\\ &= 1\times 1\times 1 = 1 \quad \text{since} \quad (V_1,V_2) \quad \text{is quasi-even}\end{aligned}$$

If $r \equiv \pm 3 \pmod 8$, then

$$\begin{aligned}\left(\frac{2d}{r}\right) &= \left(\frac{2}{r}\right)\prod_{i=1}^{s}\left(\frac{p_i}{r}\right)\\ &= (-1)\times(1)^{\#\{p\in V_1:\overline{pr}\notin E(G(n))\}}\times(-1)^{\#\{p\in V_1:\overline{pr}\in E(G(n))\}}\\ &= -1\times 1\times -1 = 1 \quad \text{since} \quad (V_1,V_2) \quad \text{is quasi-even}\end{aligned}$$

Therefore, $C_{2d}(\mathbb{Q}_r) \neq \emptyset$ for $r \in V_2$ by Lemma 2.1.1 (3). Note also that $C_{2d}(\mathbb{Q}_2) \neq \emptyset$ by Lemma 2.1.1 (6), since $d \equiv 1 \pmod 4$. Therefore, $2d \in S_n$.

□

Lemma 2.2.5. *Let n be as in Lemma 2.2.4. Suppose d is odd and $2d \in S_n$, by remark 2.2.2 and Lemma 2.1.1 we may assume $2d = 2\cdot p_1 \cdots p_s \in S_n$ for some s, $1 \leq s \leq t$. Then, letting $V_1 = \{p_1, \ldots p_s\}$ and $V_2 = \{p_{s+1}, \ldots p_t, q_1 \ldots q_l\}$, (V_1, V_2) is a quasi-even partition of $V(G(n))$.*

Proof. Suppose $2d = 2 \cdot p_1 \cdots p_s$ is a member of S_n. By definition,

$$C_{2d}(\mathbb{Q}_p) \neq \emptyset \ \ \forall p|2n \text{ and } C_{2d}(\mathbb{Q}_\infty) \neq \emptyset$$

Using Lemma 2.1.1 (1) we have $2d > 0$. From Lemma 2.1.1 (2), for $p|d$, $\left(\frac{n/2d}{p}\right) = 1$. Therefore, for $1 \leq i \leq s$. If $p_i \equiv 1 \pmod 8$, then

$$\begin{aligned} 1 = \left(\frac{n/2d}{p_i}\right) &= \left(\frac{2}{p_i}\right) \prod_{r \in V_2} \left(\frac{r}{p_i}\right) \\ &= (1) \times (1)^{\#\{r \in V_2 : \overline{p_i r} \notin E(G(n))\}} \times (-1)^{\#\{r \in V_2 : \overline{p_i r} \in E(G(n))\}} \\ &\Rightarrow \quad \#\{p_i \to V_2\} \quad \text{is even} \end{aligned}$$

If $p_i \equiv 5 \pmod 8$, then

$$\begin{aligned} 1 = \left(\frac{n/2d}{p_i}\right) &= \left(\frac{2}{p_i}\right) \prod_{r \in V_2} \left(\frac{r}{p_i}\right) \\ &= (-1) \times (1)^{\#\{r \in V_2 : \overline{p_i r} \notin E(G(n))\}} \times (-1)^{\#\{r \in V_2 : \overline{p_i r} \in E(G(n))\}} \\ &\Rightarrow \quad \#\{p_i \to V_2\} \quad \text{is odd} \end{aligned}$$

Similarly, Lemma 2.1.1 (3) gives $\left(\frac{2d}{r}\right) = 1$ for $r|2n/d$. So that, for $1 \leq i \leq s$ and $r \in V_2$, If $r \equiv \pm 1 \pmod 8$, then

$$\begin{aligned} 1 = \left(\frac{2d}{r}\right) &= \left(\frac{2}{r}\right) \prod_{i=1}^{s} \left(\frac{p_i}{r}\right) \\ &\Rightarrow \#\{r \to V_1\} \quad \text{is even} \end{aligned}$$

If $r \equiv \pm 3 \pmod 8$, then

$$\begin{aligned} 1 = \left(\frac{2d}{r}\right) &= \left(\frac{2}{r}\right) \prod_{i=1}^{s} \left(\frac{p_i}{r}\right) \\ &\Rightarrow \#\{r \to V_1\} \quad \text{is odd} \end{aligned}$$

Thus, (V_1, V_2) is a quasi-even partition of $V(G(n))$.

□

Thus far it has been shown, if n is an odd, squarefree, positive integer and (V_1, V_2) is an even partition of $V(G(n))$ such that V_1 contains no prime factors which are 3 modulo 4, then $d = \prod_{p \in V_1} p \in S_n$. Moreover, suppose d is odd and $d \in S_n$, then it has been shown that d corresponds to such an even partition of $V(G(n))$. It has also been shown that even elements of S_n are in one to one correspondence with quasi-even partitions of $V(G(n))$. For the case when n is even we present two lemmas. These lemmas and their proofs are analogous to Lemmas 2.2.1 and 2.2.3.

Lemma 2.2.6. *Let $n \equiv 0 \pmod 2$. For every even partition, (V_1, V_2) of $V(\overline{G}(n))$ such that V_1 does not contain 2 and contains no prime factors which are 3 modulo 4 we have d in S_n, where*

$$d = \prod_{p \in V_1} p$$

Proof. The proof of this result is similar to the proof of Lemma 2.2.1.

□

Lemma 2.2.7. *Let $n = 2 \cdot p_1 \cdots p_t \cdot q_1 \cdots q_l$ with $p_i \equiv 1 \pmod 4$ and $q_j \equiv 3 \pmod 4$ for $0 \leq i \leq t$ and $0 \leq j \leq l$. Suppose d is odd and $d \in S_n$, by Lemma 2.1.3 we may assume $d = p_1 \cdots p_s \in S_n$ for some s, $1 \leq s \leq t$, then, letting $V_1 = \{p_1, \ldots p_s\}$ and $V_2 = \{2, p_{s+1}, \ldots p_t, q_1, \ldots q_l\}$, (V_1, V_2) is an even partition of $V(\overline{G}(n))$.*

Proof. The proof of this result is similar to the proof of Lemma 2.2.3.

□

Remark 2.2.8. *By Lemma 2.1.1 (3), For n odd, S_n contains the element 2 if $\left(\frac{2}{p}\right) = 1$ for all $p|n$.*

Proof of Theorem 2.0.8 (1) By remark 2.2.2, we need only consider partititions (V_1, V_2) of $V(G(n))$ for which V_1 contains no primes which are congruent to 3 modulo 4 in order to determine the elements of S_n. By Lemmas 2.2.1 and 2.2.3, the odd positive elements of

S_n are in one to one correspondence with the even partitions (V_1, V_2) of $G(n)$ for which V_1 contains no primes which are congruent to 3 modulo 4. Therefore, the first set appearing in formula one counts the odd positive elements of S_n. By Lemmas 2.2.4 and 2.2.5, the even positive elements of S_n are in one to one correspondence with the quasi-even partitions (V_1, V_2) of $G(n)$ for which V_1 contains no primes which are congruent to 3 modulo 4. Therefore, the second set appearing in the formula counts the even positive elements of S_n. By Lemma 2.1.1 (1) S_n contains no negative elements.

□

Proof of Theorem 2.0.8 (2) If $n \equiv \pm 3 \pmod 8$, then using Lemma 2.1.1 (5) or Lemma 2.1.3 (2), we see S_n contains no even elements. So, preceding as in the proof of (1) yields the result.

□

Proof of Theorem 2.0.8 (3) Suppose n contains no prime factors which are ± 3 modulo 8. By remark 2.2.8, $2 \in S_n$. Therefore, $2d \in S_n$ if and only if $d \in S_n$. To see this, note that if $2, 2d \in S_n$ then $2 \cdot 2d \equiv d \pmod{(\mathbb{Q}^*)^2} \in S_n$. By Lemma 2.1.3 (2), S_n contains no negative elements. Thus, $|S_n|$ is twice the number of odd positive elements which we count as in (1).

□

Proof of Theorem 2.0.8 (4) If $n \equiv \pm 0 \pmod 2$, then using Lemma 2.1.3 (2), we see S_n contains no even elements. So, using Lemmas 2.2.6 and 2.2.7 we may precede as in the proof of (1).

□

2.3 Proof of Theorem 2.0.12

For S'_n we consider three cases: $n \equiv \pm 3 \pmod 8$, $n \equiv \pm 1 \pmod 8$, and n even. For each case we state and prove a pair of lemmas which establish a one to one correspondence between even partitions and group elements. Then using the two lemmas we prove parts (1), (2), and (3) of Theorem 2.0.12.

Lemma 2.3.1. *Let $n = p_1 \cdots p_t \cdot q_1 \cdots q_l \equiv \pm 3 \pmod 8$ with $p_i \equiv 1 \pmod 4$ and $q_j \equiv 3 \pmod 4$ for $0 \leq i \leq t$ and $0 \leq j \leq l$ (t,l not both zero). Suppose that the partition (V_1, V_2) of $V(g(n))$ is even. Then d, $n/d \in S'_n$ where $d = \prod_{p \in V_1} p$ and $n/d = \prod_{p \in V_2} p$.*

Proof. Since $n \equiv \pm 3 \pmod 8$, n has an odd number of prime factors which are ± 3 modulo 8. Suppose that (V_1, V_2) is an even partition of $V(g(n))$. Then either V_1 or V_2 contains an even number of primes which are congruent to ± 3 modulo 8. Without loss of generality, we will assume that V_1 contains an even number of primes which are congruent to ± 3 modulo 8. Let $d = \prod_{p \in V_1} p$. We must show that $C'_d(\mathbb{Q}_p) \neq \emptyset$ for $p|2n$. First, consider the case $p = 2$. We have, $d \equiv \pm 1 \pmod 8$ and Lemma 2.1.2 (3) gives that $C'_d(\mathbb{Q}_2) \neq \emptyset$. We note that for $q|n$, $q \equiv 3 \pmod 4$ $C'_d(\mathbb{Q}_q) \neq \emptyset$, by Lemma 2.1.2 (1) and (2). Second, consider the case $p|d$. If $p \equiv 1 \pmod 4$ then since $\#\{p \to V_2\} \equiv 0 \pmod 2$ we have

$$\left(\frac{n/d}{p}\right) = \prod_{r \in V_2} \left(\frac{r}{p}\right)$$
$$= (1)^{\#\{r \in V_2 : \overrightarrow{pr} \notin E(g(n))\}} \times (-1)^{\#\{r \in V_2 : \overrightarrow{pr} \in E(g(n))\}} = 1$$

For $p|n/d$. If $p \equiv 1 \pmod 4$ then since $\#\{p \to V_1\} \equiv 0 \pmod 2$, we have

$$\left(\frac{d}{p}\right) = \prod_{r \in V_1} \left(\frac{r}{p}\right)$$
$$= (1)^{\#\{r \in V_2 : \overrightarrow{pr} \notin E(g(n))\}} \times (-1)^{\#\{r \in V_2 : \overrightarrow{pr} \in E(g(n))\}} = 1$$

Hence, by Lemma 2.1.2 (1) and (2), $d \in S'_n$. A similiar argument shows that $n/d \in S'_n$.

□

Lemma 2.3.2. *Let n be as in Lemma 2.3.1. Suppose $d = p_1 \cdots p_s \cdot q_1 \cdots q_r \in S'_n$ for $0 \leq s \leq t$ and $0 \leq r \leq l$. Let $V_1 = \{p_1, \ldots, p_s, q_1, \ldots q_r\}$ and $V_2 = \{p_{s+1}, \ldots p_t, q_{r+1}, \ldots q_l\}$. Then (V_1, V_2) is an even partition of $V(g(n))$.*

Proof. By definition, $d \in S'_n$ if

$$C'_d(\mathbb{Q}_p) \neq \emptyset \ \ \forall p|2n \text{ and } C'_d(\mathbb{Q}_\infty) \neq \emptyset$$

Since $n \equiv \pm 3 \pmod 8$ one of d or $n/d \equiv \pm 1 \pmod 8$. Without loss of generality, suppose $d \equiv \pm 1 \pmod 8$, then by Lemma 2.1.2 (3), $C'_d(\mathbb{Q}_2) \neq \emptyset$. From Lemma 2.1.2 (1), for $p|d$, if $p \equiv 1 \pmod 4$ and $C'_d(\mathbb{Q}_p) \neq \emptyset$, then $\left(\frac{n/d}{p}\right) = 1$. Thus we have,

$$\begin{aligned} 1 = \left(\frac{n/d}{p}\right) &= \prod_{q \in V_2} \left(\frac{q}{p}\right) \qquad p \in V_1 \\ &= (1)^{\#\{r \in V_2 : \overrightarrow{pr} \notin E(g(n))\}} \times (-1)^{\#\{r \in V_2 : \overrightarrow{pr} \in E(g(n))\}} \\ &\Rightarrow \#\{p \to V_2\} \quad \text{is even for} \quad p \in V_1, p \equiv 1 \pmod 4 \end{aligned}$$

Also, Lemma 2.1.2 (2) gives $\left(\frac{d}{p}\right) = 1$ for $p|n/d$, if $p \equiv 1 \pmod 4$. Then we have,

$$\begin{aligned} 1 = \left(\frac{d}{p}\right) &= (1)^{\#\{r \in V_1 : \overrightarrow{pr} \notin E(g(n))\}} \times (-1)^{\#\{r \in V_1 : \overrightarrow{pr} \in E(g(n))\}} \\ &\Rightarrow \#\{p \to V_1\} \equiv 0 \pmod 2 \text{ for } p \in V_2,\ p \equiv 1 \pmod 4 \end{aligned}$$

Since there are no edges beginning at $q_1, \ldots q_l$, (V_1, V_2) is an even partition of $V(g(n))$.

□

Proof of Theorem 2.0.12 (1). Let n be as in Lemma 2.3.1. By Lemma 2.3.1 we have for *any* even partition of $g(n)$, say (V_1, V_2),

$$\prod_{p \in V_1} p \in S'_n \quad \text{and} \quad \prod_{p \in V_2} p \in S'_n$$

So, by Lemma 2.3.2, odd positive $d \in S'_n$ are in one to one correspondence with even partitions of $V(g(n))$. By Lemma 2.1.2, there are no even elements in S'_n. Also, $-1 \in S'_n$, so that $d \in S'_n$ if and only if $-d \in S'_n$. Therefore, $|S'_n| = 2 \cdot \#\{(V_1, V_2) \vdash_e g(n)\}$.

□

Lemma 2.3.3. *Let $n = p_1 \cdots p_t \cdot q_1 \cdots q_l \equiv \pm 1 \pmod 8$ with $p_i \equiv 1 \pmod 4$ and $q_j \equiv 3 \pmod 4$ for $0 \leq i \leq t$ and $0 \leq j \leq l$ (t,l not both zero). If (V_1, V_2) is an even partition of $V(G(-n))$ then $\prod_{p \in V_1} p \in S'_n$ and $\prod_{p \in V_2} p \in S'_n$, where p is prime or -1.*

Proof. Suppose we have an even partition, (V_1, V_2), of $V(G(-n))$. Notice that -1 is necessarily in one of V_1 or V_2 so that both V_1 and V_2 have an even number of primes (counting -1 as a prime) which are $\pm 3 \pmod 8$. This gives $\mathbb{Q}_2$ solutions on C'_d by Lemma 2.1.2 (3), if $d = \prod_{p \in V_1} p$ or $d = \prod_{p \in V_2} p$. We may proceed just as in Lemma 2.3.1 to finish the proof.

□

Lemma 2.3.4. *Let n be as in Lemma 2.3.3 and assume d is odd. If $d \in S'_n$ and V_1 is the set of prime divisors of d along with -1, if $d < 0$, then (V_1, V_2) is an even partition of $V(G(-n))$. Where $V_2 = V(G(-n)) - V_1$.*

Proof. Suppose $d \in S'_n$. Let V_1 be the set of prime divisors of d along with -1, if $d < 0$. Let V_2 be the set of prime divisors of n/d along with -1, if $d > 0$. Since $d \in S'_n$, $C'_d(\mathbb{Q}_2) \neq \emptyset$. Thus, $d \equiv \pm 1 \pmod 8$ or $n/d \equiv \pm 1 \pmod 8$, by Lemma 2.1.2. Thus, V_1 and V_2 contain an even number of primes (counting -1 as a prime) which are ± 3 modulo 8, since $n \equiv \pm 1 \pmod 8$. Therefore, $\#\{-1 \to W\} \equiv 0 \pmod 2$, where $W = V_1$ or V_2 is the set not containing -1. If $p \equiv 1 \pmod 4$ and $p|d$, then Lemma 2.1.2 (2) gives

$\left(\frac{n/d}{p}\right) = 1$. Thus,

$$1 = \left(\frac{n/d}{p}\right) = \prod_{r \in V_2} \left(\frac{r}{p}\right)$$
$$= (1)^{\#\{r \in V_2 : \overrightarrow{pr} \notin E(G(-n))\}} \times (-1)^{\#\{r \in V_2 : \overrightarrow{pr} \in E(G(-n))\}}$$
$$\Rightarrow \#\{p \to V_2\} \equiv 0 \pmod 2$$

If $p \equiv 1 \pmod 4$ and $p|n/d$, then Lemma 2.1.2 (2) gives $\left(\frac{d}{p}\right) = 1$. Thus,

$$1 = \left(\frac{d}{p}\right) = (1)^{\#\{r \in V_1 : \overrightarrow{pr} \notin E(g(n))\}} \times (-1)^{\#\{r \in V_1 : \overrightarrow{pr} \in E(g(n))\}}$$
$$\Rightarrow \#\{p \to V_1\} \equiv 0 \pmod 2 \text{ for } p \in V_2,\ p \equiv 1 \pmod 4$$

Since there are no edges beginning at $q_1, \ldots q_l$, (V_1, V_2) is an even partition of $V(G(-n))$.

□

Proof of Theorem 2.0.12 (2). Even partitions of $V(G(-n))$ are in one to one correspondence with the odd elements of S'_n, by Lemma 2.3.3 and Lemma 2.3.4. By Lemma 2.1.2 (4) there are no even elements.

□

Lemma 2.3.5. *Let $n = 2 \cdot p_1 \cdots p_t \cdot q_1 \cdots q_l$ with $p_i \equiv 1 \pmod 4$ and $q_j \equiv 3 \pmod 4$ for $0 \leq i \leq t$ and $0 \leq j \leq l$ (t,l not both zero). Suppose that the partition (V_1, V_2) of $V(G'(n))$ is even. Then d, $n/d \in S'_n$ where $d = \prod_{p \in V_1} p$ and $n/d = \prod_{p \in V_2} p$.*

Proof. The proof of this result is similar to the proof of Lemma 2.3.1.

□

Lemma 2.3.6. *Let n be as in Lemma 2.3.5. If $d \in S'_n$ and V_1 is the set of prime divisors of d (along with 2, if $d \equiv 0 \pmod 2$), then (V_1, V_2) is an even partition of $V(G'(n))$. Where $V_2 = V(G'(n)) - V_1$.*

Proof. The proof of this result is similar to the proof of Lemma 2.3.2.

□

Proof of Theorem 2.0.12 (3). The previous two lemmas give a one to one correspondence between even partitions of $V(G'(n))$ and positive elements of S'_n. Since -1 is necessarily in S'_n, we multiply the number of even partitions of $V(G'(n))$ by 2.

□

2.4 Graph Theory and Linear Algebra

Definition 2.4.1. *Let G be a graph, with vertex set*

$$V(G) = \{v_1, \dots v_s\}$$

and edge set, $E(G)$. The adjacency matrix of G is defined by

$$A(G) = (a_{ij})_{1 \le i,j \le s}$$

where

$$a_{ij} = \begin{cases} 1 & \text{if } \overrightarrow{v_i v_j} \in E(G) \ (1 \le i \ne j \le s) \\ 0 & \text{otherwise} \end{cases}$$

Let

$$d_i = \sum_{j=1}^{s} a_{ij} \quad (\text{out degree of vertex } v_i \quad (1 \le i \le s))$$

Definition 2.4.2. *The Laplace matrix of G is defined by*

$$L(G) = diag(d_1, \cdots, d_s) - A(G)$$

In [13], Feng and Xiong showed,

Lemma 2.4.3. *(Feng and Xiong [13, lemma 2.2]) The number of even partitions of $V(G)$ is 2^{s-r}, where $r = \text{rank}_{\mathbb{F}_2} L(G)$.*

Recall that we want to count even partitions (V_1, V_2) of V such that there are no 3 modulo 4 primes in V_1. We require the following lemma

Lemma 2.4.4. *Suppose a graph G has vertex set, $V(G) = \{q_1, \dots q_s, p_{s+1}, \dots p_t\}$. Futhermore, suppose that $L(G) \in \mathbb{F}_2^{t\times t}$ is given by*

$$\begin{array}{c} \\ q_1 \\ q_2 \\ \vdots \\ q_s \\ p_{s+1} \\ \vdots \\ p_t \end{array} \begin{array}{c} \begin{array}{ccccccc} q_1 & q_2 & \dots & q_s & p_{s+1} & \dots & p_t \end{array} \\ \begin{pmatrix} * & * & \dots & * & * & \dots & * \\ * & * & \dots & * & * & \dots & * \\ \vdots & \vdots & \dots & \vdots & \vdots & \dots & \vdots \\ * & * & \dots & * & * & \dots & * \\ * & * & \dots & * & * & \dots & * \\ \vdots & \vdots & \dots & \vdots & \vdots & \dots & \vdots \\ * & * & \dots & * & * & \dots & * \end{pmatrix} \end{array}$$

and let l_k denote the $k-th$ column of $L(G)$, then

$$\#\{(V_1, V_2) \vdash_e V(G) | q_i \notin V_1, 0 \leq i \leq s\} = 2^{(t-s)-R}$$

where

$$R = \text{rank}_{\mathbb{F}_2}[l_{s+1}|l_{s+2}|\cdots|l_t]$$

Proof. We wish to count even partitions, (V_1, V_2), such that $q_i \notin V_1$ for $0 \leq i \leq s$. Define $v(V_1) = [g_1 \dots g_s \ g_{s+1} \dots g_t]^T$, by

$$g_k = \begin{cases} 1 & \text{if } q_k \in V_1 \ 1 \leq k \leq s \\ 0 & \text{if } q_k \notin V_1 \ 1 \leq k \leq s \\ 1 & \text{if } p_k \in V_1 \ s+1 \leq k \leq t \\ 0 & \text{if } p_k \notin V_1 \ s+1 \leq k \leq t \end{cases}$$

Following Feng and Xiong we see, $(V_1, V_2) \vdash_e V(G)$ if and only if $v(V_1) \in NS(L(G))$. Write $L(G) = [L_1 \ L_2]$ where L_1 [resp. L_2] represents the columns corresponding to q_j

for $1 \leq j \leq s$ [resp. p_i for $s+1 \leq i \leq t$]. Let $v(V_1) = \begin{bmatrix} v_1(V_1) \\ v_2(V_1) \end{bmatrix}$, where $v_1(V_1)$ [resp. $v_2(V_1)$] corresponds to q_j for $1 \leq j \leq s$ [resp. p_i for $s+1 \leq i \leq t$]. We may then write

$$\begin{aligned} L(G)v(V_1) &= [L_1 \ L_2] \begin{bmatrix} v_1(V_1) \\ v_2(V_1) \end{bmatrix} \\ &= \sum_{k=1}^{t} g_k \cdot l_k \\ &= \sum_{k=1}^{s} 0 \cdot l_k + \sum_{k=s+1}^{t} g_k \cdot l_k = L_2 v_2(V_1) \end{aligned}$$

So $L(G) \cdot v(V_1) = 0 \Leftrightarrow v_2(V_1) \in NS(L_2)$.

□

We also require the following lemma to count quasi-even partitions.

Lemma 2.4.5. *Let $\{q_1, \ldots q_s, p_{s+1}, \ldots p_t\}$ be the odd prime factors of n with $p_i \equiv 1 \pmod 4$ and $q_j \equiv 3 \pmod 4$ for $s+1 \leq i \leq t$ and $1 \leq j \leq s$. Let r_k be the prime dividing n corresponding to the k^{th} row of $L(G(n))$. We construct $b \in \mathbb{F}_2^t$ in the following way.*

$$b[k] = \begin{cases} 0 & \text{if } r_k \equiv \pm 1 \pmod 8 \\ 1 & \text{if } r_k \equiv \pm 3 \pmod 8 \end{cases}$$

Let $L = [l_{s+1}|l_{s+2}|\cdots|l_t]$, where l_k is the $k-th$ column of $L(G(n))$. Then, $Lx = b$ if and only if the partition $(\{r_i|b(i) = 0\}, \{r_i|b(i) = 1\})$ of $V(G(n))$ is quasi-even. Recall that if $Lx = b$ is solvable then, solutions to $Lx = b$ and $Lx = 0$ are in one to one correspondence. Hence, if $Lx = b$ is solvable, then

$$\#\{(V_1, V_2) \vdash_{qe} V(G(n))|q_j \notin V_1, 0 \leq j \leq s\} = 2^{(t-s)-R}$$

where

$$R = \text{rank}_{\mathbb{F}_2} L$$

On the other hand, if $Lx = b$ is not solvable, then there are no quasi-even partitions of $V(G(n))$.

Proof. Given $x \in \mathbb{F}_2^t$. Define $V_1 = \{r_i | x(i) = 1\}$ and $V_2 = \{r_i | x(i) = 0\}$. Suppose $r_k \in V_1$. Then

$$\sum_{j=1}^{t} L_{kj}x_j = \sum_{x_j=1, j=1}^{t} L_{kj} = L_{kk} + \#\{r_k \to V_1\} \equiv \#\{r_k \to V_2\} \pmod 2$$

On the other hand, if $r_k \in V_2$, then

$$\sum_{j=1}^{t} L_{kj}x_j = \sum_{x_j=1, j=1}^{t} L_{kj} \equiv \#\{r_k \to V_1\} \pmod 2$$

Hence,

$$[L(G(n))x](i) = \begin{cases} \#\{r_i \to V_2\} & \text{if } r_i \in V_1 \\ \#\{r_i \to V_1\} & \text{if } r_i \in V_2 \end{cases}$$

By definition of quasi-even it follows that

$$L(G(n))x = b \Leftrightarrow (V_1, V_2) \vdash_{qe} V(G(n))$$

□

Recall that elements belonging to S_n contain no 3 modulo 4 prime divisors. Therefore, before stating our main formulas for the selmer groups S_n and S'_n we state the following definitions.

Definition 2.4.6. *Let n be as in Lemma 2.4.5. Suppose that G is one of $G(n)$, $\overline{G}(n)$, $g(n)$, $G(-n)$, or $G'(n)$. Let l_k denote the k-th column of $L(G)$. Then we define*

$$L'(G) = \begin{cases} [l_{s+1}|l_{s+2}|\cdots|l_t] & \textit{if } G \textit{ is } G(n) \textit{ or } \overline{G}(n) \\ L(G) & \textit{otherwise.} \end{cases}$$

Definition 2.4.7. *Let n be as in Lemma 2.4.5. Let $L = L'(G)$, where G is one of $G(n)$, $\overline{G}(n)$, $g(n)$, $G(-n)$, or $G'(n)$. Let r_k be the prime corresponding to the k^{th} column of L. For $v \in \mathbb{F}_2^{(t-s)\times 1}$ we define $n(v)$ by*

$$n(v) = \prod_{j=1}^{t-s} r_j^{v[j]}$$

With the above lemmas we may now compute the Selmer groups, S_n and S'_n, using linear algebra. The following corollaries follow from Theorems 2.0.8 and 2.0.12.

Corollary 2.4.8. *Let n be squarefree. In parts 1 - 3 below, let $G = G(n)$, and in part 4, let $G = \overline{G}(n)$. Let $L = L'(G)$. Let b be as in Lemma 2.4.5 and let x_0 be a particular solution of $Lx = b$ if one exists. Let $\{b_1, b_2, \ldots b_k\}$ be a basis for $NS(L)$. Then,*

1. *If $n \equiv \pm 1 \pmod 8$ and $\exists\, p|n$, $p \equiv \pm 3 \pmod 8$, then*

$$S_n = \begin{cases} < n(b_1), n(b_2), \ldots n(b_k), n(x_0) > & \text{if } Lx = b \text{ is solvable,} \\ < n(b_1), n(b_2), \ldots n(b_k) > & \text{otherwise.} \end{cases}$$

   Thus,

$$|S_n| = \begin{cases} 2^{k+1} & \text{if } Lx = b \text{ is solvable} \\ 2^k & \text{otherwise.} \end{cases}$$

2. *If $n \equiv \pm 3 \pmod 8$, then*

$$S_n =< n(b_1), n(b_2), \ldots n(b_k) > .$$

   Thus,

$$|S_n| = 2^k.$$

3. *If $p_i \equiv 1 \pmod 8$ for all $0 \leq i \leq t$ and $q_j \equiv 7 \pmod 8$ for all $0 \leq j \leq l$, then*

$$S_n =< n(b_1), n(b_2), \ldots n(b_k), 2 > .$$

   Thus,

$$|S_n| = 2^{k+1}.$$

4. *If $n \equiv 0 \pmod 2$, then*

$$S_n =< n(b_1), n(b_2), \ldots n(b_k) > .$$

   Thus,

$$|S_n| = 2^k.$$

Proof. (1) Let $\{r_1, r_2, \ldots r_t\}$ be the odd prime factors of n For $d|n$, we define $x(d) \in \mathbb{F}^{t\times 1}$ by

$$x(d)[j] = \begin{cases} 1 & \text{if } r_j|d \\ 0 & \text{if } r_j \nmid d \end{cases}$$

Let $\{b_1, b_2, \ldots b_k\}$ be a basis for $NS(L)$. If $Lx = b$ has a solution, then denote it by x_0. Suppose $d \in S_n$. There are two cases to consider.

Case 1: *d is odd.*

Then by Lemma 2.2.3, $(\{p : p|d\}, \{p : p \nmid d\}) \vdash_e V(G(n))$ with only primes $p \equiv 1 \pmod 4$ in the first set. By the proof of Lemma 2.4.4 $L(x(d)) = 0$. Thus, $x(d) = \sum_{j=1}^{k} e_j b_j$ where $e_j \in \{0, 1\}$, which implies $d = \prod_{j=1}^{k} n(b_j)^{e_j}$ which is clearly in $< n(b_1), \ldots, n(b_k) >$.

Case 2: $d = 2d_0$.

Recall S_n contains even elements only if $Lx = b$ has solutions. By Lemma 2.2.5, $(\{p : p|d_0\}, \{p : p \nmid d_0\}) \vdash_{qe} V(G(n))$ with only primes $p \equiv 1 \pmod 4$ in the first set. By the proof of Lemma 2.4.5 $L(x(d)) = b$. Hence, $x(d) = x_0 + \sum_{j=1}^{k} e_j b_j$ where $e_j \in \{0, 1\}$ which implies $d = n(x_0) \prod_{j=1}^{k} n(b_j)^{e_j} \in < n(b_1), \ldots n(b_k), n(x_0) >$. Thus we have $S_n \subseteq < n(b_1), \ldots n(b_k) >$ or $< n(b_1), \ldots n(b_k), n(x_0) >$ depending on whether $Lx = b$ has solutions or not.

For the opposite containment there are again two cases to consider: either $Lx = b$ has solutions or not.

Case 1: *$Lx = b$ has no solutions.*

Suppose that $d \in < n(b_1), \ldots n(b_k) >$. Then $d = \prod_{j=1}^{k} n(b_j)^{e_j}$ which implies that $x(d) = \sum_{j=1}^{k} e_j b_j \in NS(L)$. By the proof of Lemma 2.4.4, we have that $(\{p : p|d\}, \{p : p \nmid d\}) \vdash_e V(G(n))$ with only primes $p \equiv 1 \pmod 4$ in the first set. Thus by Lemma 2.2.1, $d \in S_n$.

Case 2: *$Lx = b$ has solutions.*

Let x_0 be a solution to $Lx = b$. Suppose $d = \left(\prod_{j=1}^{k} n(b_j)^{e_j}\right) \times n(x_0)$ which implies that

$x(d) = x_0 + \sum_{j=1}^{k} e_j b_j$. Thus, $L(x(d)) = L(x_0) + \sum_{j=1}^{k} e_j L b_j = b$. Thus by the proof of Lemma 2.4.5, $(\{p : p|d\}, \{p : p \not| d\} \vdash_{qe} V(G(n))$ with only primes $p \equiv 1 \pmod 4$ in the first set. Thus by Lemma 2.2.4, $2d \in S_n$.

Proofs of (2),(3), and (4) are similiar.

□

Corollary 2.4.9. *Let n be as in Lemma 2.4.5. Then,*

1. *Let $\{b_1, b_2, \ldots b_k\}$ be a basis for $NS(L(g(n)))$. If $n \equiv \pm 3 \pmod 8$, then*

$$S'_n =< n(b_1), n(b_2), \ldots n(b_k), -1 > .$$

Thus,

$$|S'_n| = 2^{t+1-\text{rank}_{\mathbb{F}_2} L(g(n))} = 2^{k+1}.$$

2. *Let $\{b_1, b_2, \ldots b_k\}$ be a basis for $NS(L(G(-n)))$. If $n \equiv \pm 1 \pmod 8$, then*

$$S'_n =< n(b_1), n(b_2), \ldots n(b_k) > .$$

Thus,

$$|S'_n| = 2^{t+1-\text{rank}_{\mathbb{F}_2} L(G(-n))} = 2^{k}.$$

3. *Let $\{b_1, b_2, \ldots b_k\}$ be a basis for $NS(L(G'(n)))$. If $n \equiv 0 \pmod 2$, then*

$$S'_n =< n(b_1), n(b_2), \ldots n(b_k), -1 > .$$

Thus,

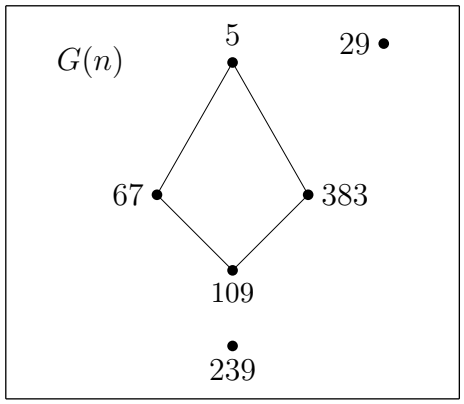
$$|S'_n| = 2^{t+2-\text{rank}_{\mathbb{F}_2} L(G'(n))} = 2^{k+1}.$$

Proof. Similiar to corollary 2.4.8.

□

2.5 An Example

Let $n = 67 \cdot 383 \cdot 239 \cdot 5 \cdot 29 \cdot 109$ and notice $n \equiv (3)(7)(7)(5)(5)(5) \equiv 7 \pmod 8$. From Lemma 2.4.5 $b = [1\ 0\ 0\ 1\ 1\ 1]^t$ and $L(G(n))x = b$ is not solvable. Hence, there are no quasi-even partitions of $V(G(n))$. Thus, by Theorem 2.0.8 the elements of S_n are in one to one correspondence with the even partitions, (V_1, V_2) of $G(n)$ for which V_1 contains no primes which are 3 modulo 4. Such even partitions of $G(n)$ are given below.



$(\{29\}, \{5, 109, 67, 383, 239\})$
$(\{5, 109\}, \{29, 67, 383, 239\})$
$(\{5, 29, 109\}, \{67, 383, 239\})$
$(\emptyset, \{5, 29, 109, 67, 383, 239\})$

$$L(G(n)) = \begin{array}{c} \\ 67 \\ 383 \\ 239 \\ 5 \\ 29 \\ 109 \end{array} \begin{array}{c} \begin{array}{cccccc} 67 & 383 & 239 & 5 & 29 & 109 \end{array} \\ \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix} \end{array}$$

Here $\dim(NS([\ l_4 \mid l_5 \mid l_6\ ])) = 2$, so that

$$|S_n| = \#\{(V_1, V_2) \vdash_e V(G(n)) \mid q_i \notin V_1,\ 1 \leq i \leq s\} = 2^2$$

Notice that a basis for $NS([\ l_4 \mid l_5 \mid l_6\ ])$ is

$$\left\{ \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\}$$

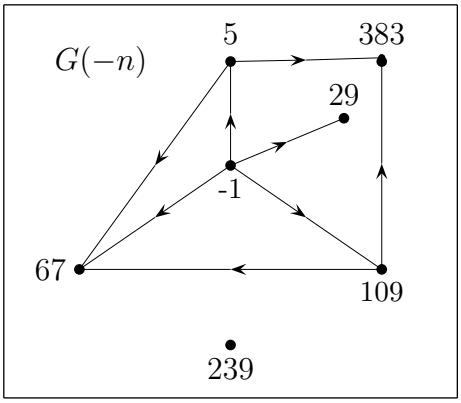
Let $v_1 = [1, 0, 1]^t$ and $v_2 = [0, 1, 0]^t$ and define

$$n(v_i) = \prod_{j=1}^{3} p_j^{v_i[j]}$$

where $p_1 = 5$, $p_2 = 29$, and $p_3 = 109$. Then $n(v_1) = 5^1 \times 29^0 \times 109^1$ and $n(v_2) = 5^0 \times 29^1 \times 109^0$. Finally, observe that

$$S_n =< n(v_1), n(v_2) > .$$

Thus, our basis for $NS([\ l_4 \mid l_5 \mid l_6\ ])$ corresponds in a natural way to generators of S_n. By Lemma 2.1.2 S_n' contains only odd elements. Thus, by Theorem 2.0.12 the elements of S_n' are in one to one correspondence with the even partitions, (V_1, V_2) of $G(-n)$. The graph, $G(-n)$ is given below.



$$L(G(-n)) = \begin{array}{c} \\ 67 \\ 383 \\ 239 \\ 5 \\ 29 \\ 109 \\ -1 \end{array} \begin{array}{c} \begin{array}{ccccccc} 67 & 383 & 239 & 5 & 29 & 109 & -1 \end{array} \\ \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix} \end{array}$$

Here $\dim(NS(L(G(-n)))) = 5$, so that

$$|S'_n| = \#\{(V_1, V_2) \vdash_e V(G(-n))\} = 2^5$$

Notice that a basis for $NS(L(G(-n)))$ is

$$\left\{ \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \right\}$$

Let

$$v_1 = [1, 1, 0, 1, 0, 0, 0]^t$$

$$v_2 = [1, 1, 0, 0, 1, 0, 0]^t$$

$$v_3 = [1, 1, 0, 0, 0, 1, 0]^t$$

$$v_4 = [0, 0, 0, 0, 0, 0, 1]^t$$

$$v_5 = [0, 0, 1, 0, 0, 0, 0]^t.$$

Define

$$n(v_i) = \prod_{j=1}^{7} p_j^{v_i[j]}$$

where $p_1 = 67$, $p_2 = 383$, $p_3 = 239$, $p_4 = 5$, $p_5 = 29$, $p_6 = 109$, and $p_7 = -1$. Then

$$n(v_1) = 67^1 \times 383^1 \times 239^0 \times 5^1 \times 29^0 \times 109^0 \times -1^0$$

$$n(v_2) = 67^1 \times 383^1 \times 239^0 \times 5^0 \times 29^1 \times 109^0 \times -1^0$$

$$n(v_3) = 67^1 \times 383^1 \times 239^0 \times 5^0 \times 29^0 \times 109^1 \times -1^0$$

$$n(v_4) = 67^0 \times 383^0 \times 239^0 \times 5^0 \times 29^0 \times 109^0 \times -1^1$$

$$n(v_5) = 67^0 \times 383^0 \times 239^1 \times 5^0 \times 29^0 \times 109^0 \times -1^0$$

Finally, observe that

$$S'_n =< n(v_1), \ldots n(v_5) > .$$

Thus, our basis for $NS(L(G(-n))$ corresponds in a natural way to generators of S'_n.

CHAPTER 3

Average Frobenius Distributions for Elliptic Curves over Abelian Extensions

Let E be an elliptic curve defined over a Galois number field K. Set $n = [K : \mathbb{Q}]$ and denote by $\mathcal{O}_K$ the ring of integers of K. Let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$ of degree f which lies above the rational prime p in $\mathbb{Z}$. We denote the degree of a prime in $\mathcal{O}_K$ as $\deg_K(\mathfrak{p})$. If E has good reduction modulo $\mathfrak{p}$, then we consider E over the finite field $\mathcal{O}_K/\mathfrak{p}$. Let $a_\mathfrak{p}(E)$ be the trace of the Frobenius morphism. The number of points on E over $\mathcal{O}_K/\mathfrak{p}$ is

$$\#E(\mathcal{O}_K/\mathfrak{p}) = N(\mathfrak{p}) + 1 - a_\mathfrak{p}(E)$$

where the norm of $\mathfrak{p}$, $N(\mathfrak{p}) = p^f$ is the number of elements of $\mathcal{O}_K/\mathfrak{p}$, and $a_\mathfrak{p}(E)$ satisfies the Hasse bound

$$|a_\mathfrak{p}(E)| \leq 2\sqrt{N(\mathfrak{p})} = 2p^{f/2}.$$

Let $r \in \mathbb{Z}$. If $f|[K : \mathbb{Q}]$, define

$$\pi_E^{r,f}(x) = \#\{\mathfrak{p} \ : \ N(\mathfrak{p}) \leq x, \, deg_K(\mathfrak{p}) = f, \text{ and } a_\mathfrak{p}(E) = r\}.$$

Recall that in the case that $K = \mathbb{Q}$ Lang and Trotter [26] conjectured

Conjecture 3.0.1. *Except for the case where $r = 0$ and E has complex mulitplication, there is a constant $C_{E,r}$ such that*

$$\pi_E^{r,1}(x) \sim C_{E,r}\frac{\sqrt{x}}{\log x} \qquad as \ x \to \infty.$$

Very little is known about the Lang-Trotter conjecture. In [11] Elkies found that for any elliptic curve E over $\mathbb{Q}$, there are infinitely many primes p such that $a_p(E) = 0$, but there are no other results of this type with $a_p(E) \neq 0$. There are several average results. For the case $K = \mathbb{Q}$ denote by $E_{(a,b)}$ the ellipitic curve $Y^2 = X^3 + aX + b$ with

$a, b \in \mathbb{Z}$. Define

$$\pi^r_{E_{(a,b)}}(x) = \#\{p \leq x \mid a_p(E_{(a,b)}) = r\}.$$

It was shown by Murty and Fouvry [15] that for $r = 0$, Lang and Trotter's conjecture holds on average, i.e. as $x \to \infty$

$$\frac{1}{4AB} \sum_{\substack{|a|\leq A \\ |b|\leq B}} \pi^0_{E_{(a,b)}}(x) \sim C_0 \frac{\sqrt{x}}{\log x}$$

where C_0 is an explicit non-zero constant. As in [26] define

$$\pi_{1/2}(x) = \int_2^x \frac{\mathrm{d}t}{2\sqrt{t}\log t} \sim \frac{\sqrt{x}}{\log x}.$$

David and Pappalardi [7] extended Murty and Fouvry's result by proving

Theorem 3.0.2. *Let r be an integer, $A, B \geq 1$. For every $c > 0$, we have*

$$\frac{1}{4AB} \sum_{|a|\leq A, |b|\leq B} \pi^r_{E(a,b)}(x) = C_r \pi_{1/2}(x) + \mathrm{O}\left(\left(\frac{1}{A} + \frac{1}{B}\right) x^{3/2} + \frac{x^{5/2}}{AB} + \frac{\sqrt{x}}{\log^c x}\right)$$

where

$$C_r := \frac{2}{\pi} \prod_{l|r} \left(1 - \frac{1}{l^2}\right)^{-1} \prod_{l\nmid r} \frac{l(l^2 - l - 1)}{(l-1)(l^2-1)}.$$

The constants in the O*- symbol depend only on c and r.*

This gives

Corollary 3.0.3. *Let $\epsilon > 0$. If $A, B > x^{1+\epsilon}$, we have as $x \to \infty$,*

$$\frac{1}{4AB} \sum_{|a|\leq A,\ |b|\leq B} \pi^r_{E(a,b)}(x) \sim C_r \frac{\sqrt{x}}{\log x}.$$

In [2] Baier slightly improves David and Pappalardi's results by proving

Theorem 3.0.4. *Let r be a fixed integer and $A, B \geq 1$. Then, for every $c > 0$, we have*

$$\frac{1}{4AB} \sum_{|a|\leq A, |b|\leq B} \pi^r_{E(a,b)}(x) = C_r \pi_{1/2}(x) + \mathrm{O}\left(\left(\frac{1}{A} + \frac{1}{B}\right) x \log x + \frac{x^{5/4} \log^3 x}{\sqrt{AB}} + \frac{\sqrt{x}}{\log^c x}\right)$$

and

Corollary 3.0.5. *Let $\epsilon > 0$. If $A, B > x^{1/2+\epsilon}$ and $AB > x^{3/2+\epsilon}$, we have as $x \to \infty$,*

$$\frac{1}{4AB} \sum_{|a|\leq A,\ |b|\leq B} \pi^r_{E(a,b)}(x) \sim C_r \frac{\sqrt{x}}{\log x}.$$

In [22] James considers the average value of $\pi^r_E(x)$ as E ranges over elliptic curves with a rational point of order 3 and proves

Theorem 3.0.6. *Let $E_{(a_1,a_3)}$ be the parameterization of elliptic curves which have a rational point of order 3 and let $r \equiv 0, 1 \pmod 3$. Then for every $c > 0$,*

$$\frac{1}{\mu(N)} \sum_{|a_1|,|a_3|\leq N}{}' \pi^r_{E_{a_1,a_3}}(x) = C_r \pi_{1/2}(x) + \mathrm{O}\left(\frac{x^{3/2}}{N} + \frac{x^{5/2}}{N^2} + \frac{\sqrt{x}}{\log^c x}\right)$$

with

$$C_r = \frac{2}{\pi} \cdot C_r(3) \cdot \prod_{\substack{q\neq 3 \\ q\nmid r}} \frac{q(q^2-q-1)}{(q+1)(q-1)^2} \prod_{\substack{q\neq 3 \\ q\nmid r}} \frac{q^2}{q^2-1},$$

where

$$C_r(3) := \begin{cases} 3/2 & \text{if } r \equiv 0 \pmod 3, \\ 0 & \text{if } r \equiv 1 \pmod 3 \end{cases}$$

and $\mu(N)$ denotes the number of $(|a_1|, |a_3|) \leq N$ such that $E_{(a_1,a_3)}$ is nonsingular and $\sum'$ denotes the sum over such curves.

which gives

Corollary 3.0.7. *Let $\epsilon > 0$. If $N > x^{1+\epsilon}$, then for $r \equiv 0, 1 \pmod 3$ we have*

$$\frac{1}{\mu(N)} \sum_{|a_1|,|a_3|\leq N}{}' \pi_{E_{a_1,a_3}}(x) \sim C_r \frac{\sqrt{x}}{\log x}.$$

In [3] Battista, Bayless, Ivanov, and James consider the average value of $\pi_E^r(x)$ as E ranges over elliptic curves with a rational point of order m for $m \in \{5, 7, 9\}$ and prove

Theorem 3.0.8. *Let $E(s)$ be the parameterization of elliptic curves having a point of order $m \in \{5, 7, 9\}$. Then, for any $c > 0$, we have*

$$\frac{1}{\mu(N)} \sum_{|s| \leq N}{}' \pi^r_{E_{(s)}}(x) = \frac{2}{\pi} C_{r,m} \pi_{1/2}(x) + \mathrm{O}\left(\frac{x^{3/2}}{N} + \frac{\sqrt{x}}{\log^c x} \right)$$

where $\sum'$ represents the sum over nonsingular curves, $\mu(N)$ represents the number of curves in the sum,

$$C_{r,m} = C_r(m) \prod_{\substack{q \nmid m \\ q \nmid r}} \frac{q(q^2 - q - 1)}{(q+1)(q-1)^2} \prod_{\substack{q \nmid m \\ q \mid r}} \frac{q^2}{q^2 - 1},$$

and

$$C_r(m) = \begin{cases} 5/4 & \text{if } m = 5 \text{ and } r \equiv 0, 3, 4 \pmod 5, \\ 7/6 & \text{if } m = 7 \text{ and } r \equiv 0, 3, 4, 5, 6 \pmod 7, \\ 3/2 & \text{if } m = 9 \text{ and } r \equiv 0, 3, 6 \pmod 9. \end{cases}$$

which gives

Corollary 3.0.9. *For any $\epsilon > 0$, select $N > x^{1+\epsilon}$. Assuming the notation from Theorem 3.0.8, we have for any $c > 0$,*

$$\frac{1}{\mu(N)} \sum_{|s| \leq N}{}' \pi^r_{E_{(s)}}(x) \sim \frac{2}{\pi} C_{r,m} \frac{\sqrt{x}}{\log x}.$$

There are more general versions of Lang and Trotter's conjecture. For a fixed $r \in \mathbb{Z}$ and fixed curves $E_1, E_2, \ldots, E_N$, define

$$\pi^r_{E_1, \ldots, E_N} = \#\{p \leq x : a_p(E_1) = \ldots a_p(E_N) = r\}.$$

Conjecture 3.0.10. *Suppose $E_1, \ldots, E_N$ are not $\overline{\mathbb{Q}}$-isogenous. Except for the case $r = 0$ and $E_1, \ldots, E_N$ have complex multiplication,*

$$\pi^r_{E_1,\ldots,E_N} \sim \begin{cases} C_{E_1,r}\frac{\sqrt{x}}{\log x} & \text{if } N = 1; \\ C_{E_1,E_2,r}\log\log x & \text{if } N = 2; \\ \text{is finite} & \text{if } N > 2. \end{cases}$$

For the supersingular case ($r = 0$) and $N = 2$, Murty and Fouvry [14] have the following result

Theorem 3.0.11. *For every positive ϵ, we have for $x \to \infty$, the asymptotic relation*

$$\sum_{|a|\leq A}\sum_{|a'|\leq A'}\sum_{|b|\leq B}\sum_{|b'|\leq B'} \pi^0_{E_{a,b},E_{a',b'}} \sim \frac{35}{96}(16AA'BB')\log\log x$$

holds uniformily for $A, A' \geq x^{\frac{1}{2}+\epsilon}$, $B, B' \geq x^{\frac{1}{2}+\epsilon}$, $AB, A'B' \geq x^{\frac{3}{2}+\epsilon}$.

Akbary, David, and Juricevic [1] computed an average of products of special values of Dirichlet L-functions to give the following result.

Theorem 3.0.12. *Let $\epsilon > 0$, and let r be an odd integer. Let A, B be positive integers with $A, B \geq x^{1+\epsilon}$. Then as $x \to \infty$,*

$$\frac{1}{16A^2B^2}\sum_{\substack{|a_1|,|a_2|\leq A \\ |b_1|,|b_2|\leq B}} \pi^r_{E_{a_1,b_1},E_{a_2,b_2}} \sim C_r \log\log x$$

where

$$C_r = \frac{3}{\pi^2}\prod_{p|r}\frac{p^2(p^2+1)}{(p^2-1)^2}\prod_{p\nmid r}\frac{p^2(p^4-2p^2-3p-1)}{(p+1)^3(p-1)^3}.$$

Recall from chapter 1 the following generalization of the Lang-Trotter conjecture to number fields.

Conjecture 3.0.13. *There exists a constant $C_{E,r,f} \in \mathbb{R}^{\geq 0}$ such that*

$$\pi_E^{r,f}(x) \sim C_{E,r,f} \begin{cases} \frac{\sqrt{x}}{\log x}, & \text{if } f = 1 \\ \log\log x, & \text{if } f = 2 \\ 1, & \text{otherwise.} \end{cases}$$

The constant $C_{E,r,f}$ can be 0, and the asymptotic relation is then interpretated to mean that there are only finitely many such primes.

In [8] David and Pappalardi prove

Theorem 3.0.14. *Let $K = \mathbb{Q}(i)$ and $\mathcal{C}_x$ denote the set of elliptic curves $E : Y^2 = X^3 + \alpha X + \beta$ with $\alpha = a_1 + a_2 i, \beta = b_1 + b_2 i \in \mathbb{Z}[i]$ and $\max\{|a_1|, |a_2|, |b_1|, |b_2|\} \leq x \log x$. Then for $r \neq 0$,*

$$\frac{1}{|\mathcal{C}_x|} \sum_{E \in C_x} \pi_E^{r,2}(x) \sim c_r \log\log x$$

where

$$c_r = \frac{1}{3\pi} \prod_{l>2} \frac{l\left(l - 1 - \left(\frac{-r^2}{l}\right)\right)}{(l-1)\left(l - \left(\frac{-1}{l}\right)\right)}.$$

If $r = 0$, then

$$\frac{1}{|\mathcal{C}_x|} \sum_{E \in \mathcal{C}_x} \pi_E^{0,2}(x) < \infty.$$

In this chapter we generalize David and Pappalardi's results to include number fields other than $\mathbb{Q}(i)$ and we allow f to be any positive integer such that $f | [K : \mathbb{Q}]$. Let $[\alpha_1, \ldots, \alpha_n]$ be an integral basis for $\mathcal{O}_K$. By an integral basis we mean that

$$\mathcal{O}_K \cong \bigoplus_{1 \leq i \leq n} \mathbb{Z}\alpha_i.$$

Then for any $A \in \mathcal{O}_K$ there exist $\vec{v} \in \mathbb{Z}^n$ such that $A = \sum_{i=1}^n \vec{v}[i]\alpha_i$. Define

$$\|\vec{v}\| := \max_{1 \leq i \leq n} \{\vec{v}[i]\}.$$

For $\vec{v} \in \mathbb{Z}^n$, define

$$A'(\vec{v}) := \sum_{i=1}^{n} \vec{v}[i]\alpha_i \in \mathcal{O}_K.$$

For $\vec{v_1}, \vec{v_2} \in (\mathbb{Z}^n)^2$, we write $E_{\vec{v_1},\vec{v_2}}$ for the elliptic curve

$$E_{\vec{v_1},\vec{v_2}} : y^2 = x^3 + A'(\vec{v_1})x + A'(\vec{v_2}).$$

Definition 3.0.15. *For a parameter $t \in \mathbb{R}$ let $\mathcal{C}_t$ be the set of elliptic curves defined over $\mathcal{O}_K$ which have Weierstrass equations*

$$E_{\vec{v_1},\vec{v_2}} : y^2 = x^3 + A'(\vec{v_1})x + A'(\vec{v_2})$$

where $\|\vec{v_1}\|, \|\vec{v_2}\| \leq t$.

Brett Tangedal points out the following fact which is a corollary to [35, Chapter 3, Theorem 3.7].

Fact 3.0.16. *Given a Galois extension $K/\mathbb{Q}$, there exists $B \in \mathbb{Z}$, such that for any rational prime $p \in \mathbb{Z}$, $[\mathcal{O}_K/\mathfrak{p} : \mathbb{Z}/p\mathbb{Z}]$ depends only on the residue class of p modulo B if and only if $K/\mathbb{Q}$ is Abelian.*

In this chapter we prove

Theorem 3.0.17. *If $K/\mathbb{Q}$ is an abelian extension of degree n, then*

1. $$\frac{1}{|\mathcal{C}_t|} \sum_{E \in \mathcal{C}_t} \pi_E^{r,1}(x) = D_{r,1,K}\pi_{1/2}(x) + \mathrm{O}\left(\frac{\sqrt{x}}{\log^c x} + \frac{x^{3/2}\log x}{t}\right)$$

2. $$\frac{1}{|\mathcal{C}_t|} \sum_{E \in \mathcal{C}_t} \pi_E^{r,2}(x) = D_{r,2,K}\log\log x + \mathrm{O}\left(1 + \frac{\sqrt{x}\log x}{t}\right)$$

3. If $f \geq 3$, then

$$\frac{1}{|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t}\pi_E^{r,f}(x) = \begin{cases} \mathrm{O}\left(1+\frac{\log^2 x}{t}\right) & \text{for } f\geq 5 \\ \mathrm{O}\left(1+\frac{\log^2 x \log\log x}{t}\right) & \text{for } f=4 \\ \mathrm{O}\left(1+\frac{x^{1/6}\log x}{t}\right) & \text{for } f=3 \end{cases}$$

where $D_{r,f,k}$ is defined as follows for $f=1,2$. Select $a_1,\dots a_l$ and B so that $deg_K(\mathfrak{p})=f$ if and only if $p\equiv a_1,\dots a_l \pmod B$ (This can be done since K/Q is Abelian.), where $\mathfrak{p}$ is a prime above the rational prime p. Then,

$$D_{r,1,K} = \frac{4n}{3\pi\phi(B)}\prod_{\substack{q,\text{odd}\\ q\nmid B\\ q\nmid r}}\frac{q(q^2-q-1)}{(q+1)(q-1)^2}\prod_{\substack{q,\text{odd}\\ q\nmid B\\ q\mid r}}\frac{q^2}{q^2-1}\sum_{i=1}^{l}k_{r,a_i,B}$$

and

$$D_{r,2,K} = \prod_{\substack{q,\text{odd}\\ q\mid B\\ q\mid r}}\left(1+\frac{\left(\frac{-1}{q}\right)-\left(\frac{-1}{q}\right)^{\mathrm{ord}_q(B)+1}q^{-2\mathrm{ord}_q(B)}}{q^2-\left(\frac{-1}{q}\right)}+\frac{\left(\frac{-1}{q}\right)^{\mathrm{ord}_q(B)+1}}{q^{2\mathrm{ord}_q(B)}\left(q-\left(\frac{-1}{q}\right)\right)}\right)$$
$$\cdot\frac{2n}{3\pi\phi(B)}\prod_{\substack{q,\text{odd}\\ q\nmid B\\ q\mid r}}\left(\frac{q}{q-\left(\frac{-1}{q}\right)}\right)\prod_{\substack{q,\text{odd}\\ q\nmid B\\ q\nmid r}}\left(1-\frac{\left(\frac{-1}{q}\right)q-1}{(q-1)(q^2-1)}\right)\sum_{i=1}^{l}c_{r,a_i,B}$$

where $k_{r,a_i,B}$ and $c_{r,a_i,B}$ are defined as follows. Let $r,A,B\in\mathbb{Z}$ with $(A,B)=1$ and r odd. Let $\Delta^{r,A}=r^2-4A$ and put

$$\mathfrak{Q}^{<}_{r,A,B} = \{q>2,\text{prime}: q|B; q\nmid r; \mathrm{ord}_q(\Delta^{r,A})<\mathrm{ord}_q(B)\} \quad \text{and}$$
$$\mathfrak{Q}^{\geq}_{r,A,B} = \{q>2,\text{prime}: q|B; q\nmid r; \mathrm{ord}_q(\Delta^{r,A})\geq\mathrm{ord}_q(B)\}$$

For $q\in\mathfrak{Q}^{<}_{r,A,B}$, we let

$$\Gamma_q = \begin{cases} \left(\frac{(\Delta^{r,A})/q^{\mathrm{ord}_q(\Delta^{r,A})}}{q}\right) & \text{if } \mathrm{ord}_q(\Delta^{r,A}) \text{ is even, positive and finite,} \\ 0 & \text{otherwise.} \end{cases}$$

then

$$k_{r,A,B}=\prod_{\substack{q,\text{odd}\\ q|B\\ q|r}}\frac{q\left(q+\left(\frac{-A}{q}\right)\right)}{q_2-1}\prod_{q\in\mathfrak{Q}^{>}_{r,A,B}}\left(\frac{q^{\lfloor\frac{\text{ord}_q(B)+1}{2}\rfloor}-1}{q^{\lfloor\frac{\text{ord}_q(B)-1}{2}\rfloor}(q-1)}+\frac{q^{\text{ord}_q(B)+2}}{q^{3\lfloor\frac{\text{ord}_q(B)+1}{2}\rfloor}(q^2-1)}\right)$$

$$\cdot\prod_{q\in\mathfrak{Q}^{<}_{r,A,B}}\left(1+\frac{q\left(\frac{\Delta^{r,A}}{q}\right)+\left(\frac{\Delta^{r,A}}{q}\right)^2+q^{-\text{ord}_q(\Delta^{r,A}/2)}(q\Gamma_q+q^2\Gamma_q^2)}{q^2-1}+\frac{\Gamma_q^2(q^{\lfloor\frac{\text{ord}_q(\Delta^{r,A})-1}{2}\rfloor}-1)}{q^{\lfloor\frac{\text{ord}_q(\Delta^{r,A})-1}{2}\rfloor}(q-1)}\right)$$

for $c_{r,A,B}$ *set* $\Delta_q=\text{ord}_q(r^2-4A^2)$, $L_q=\left(\frac{r^2-4A^2}{q}\right)$ *and put*

$$\mathfrak{P}^{\leq}_{r,A,B}=\{q>2,\text{prime}:q|B;q\nmid r;\text{ord}_q(B)\leq\Delta_q\}\quad\textit{and}$$

$$\mathfrak{P}^{>}_{r,A,B}=\{q>2,\text{prime}:q|B;q\nmid r;\text{ord}_q(B)>\Delta_q>0\}.$$

Let

$$\gamma_q=\left(\frac{\Delta/q^{\Delta_q}}{q}\right)$$

then

$$c_{r,A,B}=\prod_{\substack{q,\text{odd}\\ q|B\\ q\nmid r\\ \Delta_q=0}}\left(1+\frac{L_qq^{2\text{ord}_q(B)}-L_q^{\text{ord}_q(B)+1}}{q^{2\text{ord}_q(B)+2}-L_qq^{2\text{ord}_q(B)}}+\frac{L_q^{\text{ord}_q(B)+1}}{q-L_q}\right)$$

$$\cdot\prod_{\substack{q,\text{odd}\\ q\in\mathfrak{P}^{\leq}_{r,A,B}}}\left(1+\frac{1-q^{-3\left\lceil\frac{\text{ord}_q(B)}{2}-1\right\rceil}}{q^3-1}+\frac{(q^2+q+q^{\text{ord}_q(B)})q^{2-2\left\lceil\frac{\text{ord}_q(B)}{2}\right\rceil}}{(q+1)(q^3-1)}\right)$$

$$\prod_{\substack{q,\text{odd}\\ q\in\mathfrak{P}^{>}_{r,A,B}\\ \Delta_q\equiv1\pmod 2}}\left(\frac{1-q^{-3\lceil\Delta_q/2-1\rceil}}{q^3-1}\right)\prod_{\substack{q,\text{odd}\\ q\in\mathfrak{P}^{>}_{r,A,B}\\ \Delta_q\equiv0\pmod 2}}\left(\frac{1-q^{-3(\Delta_q/2-1)}}{q^3-1}+\right.$$

$$\left.\frac{1}{q^{3\Delta_q/2}}\left[1+\gamma_q\left[\frac{(q^{2(\text{ord}_q(B)-\Delta_q)}-\gamma_q^{\text{ord}_q(B)-\Delta_q})(q-\gamma_q)+\gamma_q^{\text{ord}_q(B)-\Delta_q}(q^2-\gamma_q)}{q^{2(\text{ord}_q(B)-\Delta_q)}(q-\gamma_q)(q^2-\gamma_q)}\right]\right]\right).$$

An immediate corollary is

Corollary 3.0.18. *With the notation from above*

1. *For* $t \gg x^{3/2}\log x$,
$$\frac{1}{|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t}\pi_E^{r,1}(x) \sim D_{r,1,K}\frac{\sqrt{x}}{\log x}.$$

2. *For* $t \gg \sqrt{x}\log x$,
$$\frac{1}{|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t}\pi_E^{r,2}(x) \sim D_{r,2,K}\log\log x.$$

3. *For* $t \gg x^{1/6}\log x$,
$$\frac{1}{|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t}\pi_E^{r,3}(x) = \mathrm{O}(1).$$

4. *For* $t \gg \log\log x\log^2 x$,
$$\frac{1}{|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t}\pi_E^{r,4}(x) = \mathrm{O}(1).$$

5. *For* $f \geq 5$ *and* $t \gg \log^2 x$,
$$\frac{1}{|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t}\pi_E^{r,f}(x) = \mathrm{O}(1).$$

In order to prove Theorem 3.0.17 we employ the following three lemmas.

Lemma 3.0.19. *Let $K/\mathbb{Q}$ be an Abelian extension. Select $a_1, \dots a_l$ and B so that $deg_K(\mathfrak{p}) = f$ if and only if $p \equiv a_1, \dots a_l \pmod{B}$, where $\mathfrak{p}$ is a prime above the rational prime p. Then*

$$\frac{1}{|\mathcal{C}_t|} \sum_{E \in \mathcal{C}_t} \pi_E^{r,f}(x)$$

$$= \frac{n}{\pi} \Bigg[\frac{1}{\sqrt{x} \log x} \sum_{i=1}^{l} \sum_{\substack{k \leq 2x^{f/2} \\ (k,2r)=1}} \frac{1}{k} \sum_{\substack{B(r) < p \leq x^{1/f} \\ k^2 | r^2 - 4p^f \\ p \equiv a_i \pmod{B}}} L(1, \chi_{d_k(p)}) \log p$$

$$- \sum_{i=1}^{l} \int_{B(r)^f}^{x} \sum_{\substack{k \leq 2S^{f/2} \\ (k,2r)=1}} \frac{1}{k} \sum_{\substack{B(r) < p \leq S^{1/f} \\ k^2 | r^2 - 4p^f \\ p \equiv a_i \pmod{B}}} L(1, \chi_{d_k(p)}) \log p \frac{\mathrm{d}}{\mathrm{dS}} \left(\frac{1}{S^{1/2} \log S} \right) \, \mathrm{dS} \Bigg] + E(x,t)$$

where

$$E(x,t) \ll \begin{cases} 1 + \frac{\log^2 x}{t} & \text{for } f \geq 5 \\ 1 + \frac{\log^2 x \log\log x}{t} & \text{for } f = 4 \\ 1 + \frac{x^{1/6} \log x}{t} & \text{for } f = 3 \\ 1 + \frac{\sqrt{x} \log x}{t} & \text{for } f = 2 \\ \log\log x + \frac{x^{3/2} \log x}{t} & \text{for } f = 1. \end{cases}$$

Lemma 3.0.20. *Suppose that $r, A, B \in \mathbb{Z}$, with r odd.*

1. *($f = 1$) Set $d_k(p) = (r^2 - 4p)/k^2$, if $k^2 | (r^2 - 4p)$ and 0 otherwise. Let $B(r) = \max\{5, r^2/4\}$. and $\chi_{d_k(p)} = \left(\frac{d_k(p)}{\bullet}\right)$. For every $c > 0$,*

$$\sum_{k \leq 2\sqrt{x}} \frac{1}{k} \sum_{\substack{B(r) < p \leq x \\ p \equiv A \pmod{B} \\ 4p \equiv r^2 \pmod{k^2}}} L(1, \chi_{d_k(p)}) \log p = K_{r,A,B} x + \mathrm{O}\left(\frac{x}{\log^c x}\right)$$

2. *($f = 2$) Set $d_k(p) = (r^2 - 4p^2)/k^2$, if $k^2 | (r^2 - 4p^2)$ and 0 otherwise. Let $B(r) = \max\{3, r, r^2/4\}$. and $\chi_{d_k(p)} = \left(\frac{d_k(p)}{\bullet}\right)$. For every $c > 0$,*

$$\sum_{\substack{k \leq 2x \\ (k, 2r) = 1}} \frac{1}{k} \sum_{\substack{B(r) < p \leq x^{1/2} \\ p \equiv A \pmod{B} \\ 4p^2 \equiv r^2 \pmod{k^2}}} L(1, \chi_{d_k(p)}) \log p = C_{r,A,B} \sqrt{x} + \mathrm{O}\left(\frac{\sqrt{x}}{\log^c x}\right)$$

where $L(s, \chi_{d_k(p)})$ is the Dirichlet L-function of $\chi_{d_k(p)}$.

We define $C_{r,A,B}$ by

$$C_{r,A,B} = \sum_{\substack{k \in \mathbb{N} \\ (k, 2r) = 1}} \frac{1}{k} \sum_{n=1}^{\infty} \frac{1}{n\phi(4nBk^2)} \sum_{a \in (\mathbb{Z}/4n\mathbb{Z})^*} \left(\frac{a}{n}\right) C_r(a, n, k)$$

where

$$C_r(a, n, k) =$$

$$\#\{b \in (\mathbb{Z}/4Bnk^2\mathbb{Z})^* : b \equiv A \pmod{B}; 4b^2 \equiv r^2 - ak^2 \pmod{4nk^2}\}.$$

We define $K_{r,A,B}$ by

$$K_{r,A,B} = \sum_{k=1}^{\infty} \frac{1}{k} \sum_{n=1}^{\infty} \frac{c_k^{r,A,B}(n)}{n\phi([B; nk^2])},$$

where

$$c_k^{r,A,B}(n) = \sum_{\substack{a \in (\mathbb{Z}/4n\mathbb{Z}) \\ a \equiv 0,1 \pmod 4 \\ (r^2 - ak^2, 4nk^2) = 4 \\ 4A \equiv r^2 - ak^2 \pmod{(4B, 4nk^2)}}} \left(\frac{a}{n}\right).$$

Lemma 3.0.21. *With the notation used in Theorem 3.0.17 and Lemma 3.0.20*

$$C_{r,A,B} = \prod_{\substack{q,\text{odd}\\ q|B\\ q|r}} \left(1 + \frac{\left(\frac{-1}{q}\right) - \left(\frac{-1}{q}\right)^{\text{ord}_q(B)+1} q^{-2\text{ord}_q(B)}}{q^2 - \left(\frac{-1}{q}\right)} + \frac{\left(\frac{-1}{q}\right)^{\text{ord}_q(B)+1}}{q^{2\text{ord}_q(B)}\left(q - \left(\frac{-1}{q}\right)\right)}\right)$$
$$\cdot \frac{2}{3\phi(B)} \prod_{\substack{q,\text{odd}\\ q\nmid B\\ q|r}} \left(\frac{q}{q - \left(\frac{-1}{q}\right)}\right) \prod_{\substack{q,\text{odd}\\ q\nmid B\\ q\nmid r}} \left(1 - \frac{\left(\frac{-1}{q}\right) q - 1}{(q-1)(q^2-1)}\right) c_{r,A,B}.$$

The organization of the rest of this chapter is as follows. Using the above three lemmas we prove Theorem 3.0.17 in section 3.1. Let $E_{A,B}$ be a curve defined over $\mathcal{O}_K/\mathfrak{p}$. After determining the number of elliptic curves in $\mathcal{C}_t$ which reduce to $E_{A,B}$ over $\mathcal{O}_K/\mathfrak{p}$ in section 3.2 we give the average in terms of Hurwitz class numbers by using Deuring's theorem in section 3.3. Then using the class formula we obtain a result in terms of L-series and prove Lemma 3.0.19. Section 3.4 is devoted to computing $C_r(a,n,k)$ defined in Lemma 3.0.20. In section 3.5 we use arguments similar to those of David and Pappalardi [8, lemma 2.2] to prove part *1* of Lemma 3.0.20. We construct a multiplicative function in section 3.6 which is a necessary tool in section 3.7 where we manipulate the double sum, $C_{r,A,B}$ defined in Lemma 3.0.20 and prove Lemma 3.0.21.

3.1 Proof of Main Theorem

In this section we prove Theorem 3.0.17. Suppose $f = 1$. We combine Lemmas 3.0.19 and 3.0.20 (2) to obtain

$$\frac{1}{|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t} \pi_E^{r,1}(x) = \frac{n}{\pi}\Bigg[\frac{1}{\sqrt{x}\log x}\sum_{i=1}^{l}\left(K_{r,a_i,B}x + \mathrm{O}\left(\frac{x}{\log^c x}\right)\right)$$
$$- \sum_{i=1}^{l}\int_{B(r)^f}^{x}\left(K_{r,a_i,B}S + \mathrm{O}\left(\frac{S}{\log^c S}\right)\right)\frac{\mathrm{d}}{\mathrm{dS}}\left(\frac{1}{S^{1/2}\log S}\right)\mathrm{dS}\Bigg]$$
$$+ \mathrm{O}\left(\log\log x + \frac{x^{3/2}\log x}{t}\right).$$

Recall the expression for $D_{r,1,K}$

$$D_{r,1,K} = \frac{4n}{3\pi\phi(B)} \prod_{\substack{q,\text{odd} \\ q\nmid B \\ q\nmid r}} \frac{q(q^2-q-1)}{(q+1)(q-1)^2} \prod_{\substack{q,\text{odd} \\ q\nmid B \\ q\mid r}} \frac{q^2}{q^2-1} \sum_{i=1}^{l} k_{r,a_i,B}.$$

In [23] James proved

$$K_{r,A,B} = \frac{2}{3\phi(B)} \prod_{\substack{q,\text{odd} \\ q\nmid B \\ q\nmid r}} \frac{q(q^2-q-1)}{(q+1)(q-1)^2} \prod_{\substack{q,\text{odd} \\ q\nmid B \\ q\mid r}} \frac{q^2}{q^2-1} k_{r,A,B}.$$

We make two observations:

1.
$$\frac{1}{\sqrt{x}\log x} \sum_{i=1}^{l} \left(K_{r,a_i,B} x + \mathrm{O}\left(\frac{x}{\log^c x} \right) \right) = \frac{\sqrt{x}}{\log x} \sum_{i=1}^{l} K_{r,a_i,B} + \mathrm{O}\left(\frac{\sqrt{x}}{\log^c x} \right)$$

2.
$$\sum_{i=1}^{l} K_{r,a_i,B} = \frac{\pi D_{r,1,K}}{2n}$$

Therefore, we may write

$$\begin{aligned} \frac{1}{|\mathcal{C}_t|} \sum_{E\in\mathcal{C}_t} \pi_E^{r,1}(x) = \frac{D_{r,1,K}}{2} \frac{\sqrt{x}}{\log x} & \\ - \frac{n}{\pi} \sum_{i=1}^{l} \int_{B(r)}^{x} \left(K_{r,a_i,B} S + \mathrm{O}\left(\frac{S}{\log^c S} \right) \right) \frac{\mathrm{d}}{\mathrm{dS}} \left(\frac{1}{S^{1/2}\log S} \right) \mathrm{dS} & \\ + \mathrm{O}\left(\frac{\sqrt{x}}{\log^c x} + \frac{x^{3/2}\log x}{t} \right). & \end{aligned}$$

Note that $\frac{\mathrm{d}}{\mathrm{dS}} \frac{1}{\sqrt{S}\log S} = -\left[\frac{1}{2S^{3/2}\log S} + \frac{1}{S^{3/2}\log^2 S} \right]$. For the O-term inside the integral we have

$$\begin{aligned} \int_2^x \left(\frac{S}{\log^c S} \right) \frac{\mathrm{d}}{\mathrm{dS}} \left(\frac{1}{S^{1/2}\log S} \right) \mathrm{dS} &= -\int_2^x \frac{S}{\log^c S} \left[\frac{1}{2S^{3/2}\log S} + \frac{1}{S^{3/2}\log^2 S} \right] \mathrm{dS} \\ &\ll \frac{1}{\log^c x}. \end{aligned}$$

Therefore,

$$\begin{aligned}\frac{1}{|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t}\pi_E^{r,1}(x) &= \frac{D_{r,1,K}}{2}\frac{\sqrt{x}}{\log x} - \frac{D_{r,1,K}}{2}\int_2^x S\frac{\mathrm{d}}{\mathrm{dS}}\left(\frac{1}{S^{1/2}\log S}\right)\,\mathrm{dS}\\ &\quad + \mathrm{O}\left(\frac{\sqrt{x}}{\log^c x} + \frac{x^{3/2}\log x}{t}\right)\\ &= \frac{D_{r,1,K}}{2}\left[\frac{\sqrt{x}}{\log x} + \int_2^x S\frac{\mathrm{d}}{\mathrm{dS}}\left(\frac{1}{S^{1/2}\log S}\right)\,\mathrm{dS}\right]\\ &\quad + \mathrm{O}\left(\frac{\sqrt{x}}{\log^c x} + \frac{x^{3/2}\log x}{t}\right)\end{aligned}$$

Recall the definition for $\pi_{1/2}(X)$

$$\pi_{1/2}(X) = \int_2^X \frac{1}{2\sqrt{S}\log S}\,\mathrm{dS}.$$

Integrating $\pi_{1/2}(x)$ by parts one obtains

$$\frac{\sqrt{x}}{\log x} = \pi_{1/2}(x) - \int_2^x \frac{\mathrm{dS}}{\sqrt{S}\log^2 S}.$$

Therefore,

$$\begin{aligned}\frac{1}{|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t}\pi_E^{r,1}(x) &= \frac{D_{r,1,K}}{2}\left[\frac{\sqrt{x}}{\log x} + \int_2^x \frac{1}{2\sqrt{S}\log S}\,\mathrm{dS} + \int_2^x \frac{1}{\sqrt{S}\log^2 S}\,\mathrm{dS}\right]\\ &\quad + \mathrm{O}\left(\frac{\sqrt{x}}{\log^c x} + \frac{x^{3/2}\log x}{t}\right)\\ &= D_{r,1,K}\pi_{1/2}(x) + \mathrm{O}\left(\frac{\sqrt{x}}{\log^c x} + \frac{x^{3/2}\log x}{t}\right).\end{aligned}$$

This completes the proof for the $f = 1$ case.

Suppose $f = 2$. Combine Lemmas 3.0.19 and 3.0.20 (1) to obtain

$$\begin{aligned}\frac{1}{|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t}\pi_E^{r,2}(x) &= \frac{n}{\pi}\left[\frac{1}{\sqrt{x}\log x}\sum_{i=1}^{l}\left(C_{r,a_i,B}\sqrt{x} + \mathrm{O}\left(\frac{\sqrt{x}}{\log^c x}\right)\right)\right.\\ &\quad \left. - \sum_{i=1}^{l}\int_{B(r)^f}\left(C_{r,a_i,B}\sqrt{S} + \mathrm{O}\left(\frac{\sqrt{S}}{\log^c S}\right)\right)\frac{\mathrm{d}}{\mathrm{dS}}\left(\frac{1}{S^{1/2}\log S}\right)\,\mathrm{dS}\right]\\ &\quad + \mathrm{O}\left(1 + \frac{\sqrt{x}\log x}{t}\right).\end{aligned}$$

It is easy to see that the first term in the brackets is O(1). Therefore we concentrate on the term containing the integral. Integrating by parts we see that

$$\begin{aligned}\int_{B(r)^f}^{x} \sqrt{S}\frac{\mathrm{d}}{\mathrm{dS}}\left(\frac{1}{S^{1/2}\log S}\right)\mathrm{dS} &= \mathrm{O}(1) - \frac{1}{2}\int_{B(r)^f}^{x}\frac{\mathrm{dS}}{S\log S}\\ &= -\log\log x + \mathrm{O}(1).\end{aligned}$$

For the O-term note that

$$\frac{\mathrm{d}}{\mathrm{dS}}\left(\frac{\sqrt{S}}{\log^c S}\right) = \frac{1}{2\sqrt{S}\log^c S} - \frac{c}{\sqrt{S}\log^{c+1} S}.$$

Integrating by parts gives

$$\begin{aligned}\int_{B(r)^f}^{x}\frac{\sqrt{S}}{\log^c S}\frac{\mathrm{d}}{\mathrm{dS}}\left(\frac{1}{S^{1/2}\log S}\right)\mathrm{dS} &= \mathrm{O}(1) - \int_{B(r)^f}^{x}\left[\frac{1}{2S\log^{c+1} S} - \frac{c}{S\log^{c+2} S}\right]\mathrm{dS}\\ &= \mathrm{O}(1).\end{aligned}$$

Therefore,

$$\frac{1}{|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t}\pi_E^{r,2}(x) = \frac{n}{\pi}\left(\sum_{i=1}^{l} C_{r,a_i,B}\right)\log\log x + \mathrm{O}\left(1 + \frac{\sqrt{x}\log x}{t}\right).$$

Recall the expression for $D_{r,2,K}$

$$\begin{aligned}D_{r,2,K} = \prod_{\substack{q,\mathrm{odd}\\ q|B\\ q|r}}\left(1 + \frac{\left(\frac{-1}{q}\right) - \left(\frac{-1}{q}\right)^{\mathrm{ord}_q(B)+1} q^{-2\mathrm{ord}_q(B)}}{q^2 - \left(\frac{-1}{q}\right)} + \frac{\left(\frac{-1}{q}\right)^{\mathrm{ord}_q(B)+1}}{q^{2\mathrm{ord}_q(B)}\left(q - \left(\frac{-1}{q}\right)\right)}\right)\\ \cdot \frac{2n}{3\pi\phi(B)}\prod_{\substack{q,\mathrm{odd}\\ q\nmid B\\ q|r}}\left(\frac{q}{q - \left(\frac{-1}{q}\right)}\right)\prod_{\substack{q,\mathrm{odd}\\ q\nmid B\\ q\nmid r}}\left(1 - \frac{\left(\frac{-1}{q}\right)q - 1}{(q-1)(q^2-1)}\right)\sum_{i=1}^{l} c_{r,a_i,B}.\end{aligned}$$

By Lemma 3.0.21

$$C_{r,A,B} = \prod_{\substack{q,\text{odd}\\ q|B\\ q|r}} \left(1 + \frac{\left(\frac{-1}{q}\right) - \left(\frac{-1}{q}\right)^{\text{ord}_q(B)+1} q^{-2\text{ord}_q(B)}}{q^2 - \left(\frac{-1}{q}\right)} + \frac{\left(\frac{-1}{q}\right)^{\text{ord}_q(B)+1}}{q^{2\text{ord}_q(B)}\left(q - \left(\frac{-1}{q}\right)\right)}\right)$$

$$\cdot \frac{2}{3\phi(B)} \prod_{\substack{q,\text{odd}\\ q\nmid B\\ q|r}} \left(\frac{q}{q - \left(\frac{-1}{q}\right)}\right) \prod_{\substack{q,\text{odd}\\ q\nmid B\\ q\nmid r}} \left(1 - \frac{\left(\frac{-1}{q}\right) q - 1}{(q-1)(q^2-1)}\right) c_{r,A,B},$$

which gives

$$\sum_{i=1}^{l} C_{r,a_i,B} = \frac{\pi D_{r,2,K}}{n}.$$

Therefore,

$$\frac{1}{|\mathcal{C}_t|} \sum_{E\in\mathcal{C}_t} \pi_E^{r,2}(x) = D_{r,2,K} \log\log x + \mathrm{O}\left(1 + \frac{\sqrt{x}\log x}{t}\right).$$

This completes the proof for the $f = 2$ case.

Suppose $f \geq 3$. By (3.8) and (3.9) from Section 3.3.

$$\frac{1}{|\mathcal{C}_t|} \sum_{E\in\mathcal{C}_t} \pi_E^{r,f}(x) = \frac{n}{2f} \sum_{\substack{B(r)<p\leq x^{1/f}\\ g(p)=n/f}} \frac{H(4p^f - r^2)}{p^f} + E(x,t) \tag{3.1}$$

and

$$E(x,t) \ll \begin{cases} 1 + \frac{\log^2 x}{t} & \text{for } f \geq 5 \\ 1 + \frac{\log\log x \log^2 x}{t} & \text{for } f = 4 \\ 1 + \frac{x^{1/6}\log x}{t} & \text{for } f = 3. \end{cases}$$

We use $H(4p^f - r^2) \ll p^{f/2}\log^2 p$ (see pg. 75) to see that the main term of (3.1) is

$$\sum_{B(r)<p\leq x^{1/f}} \frac{H(4p^f - r^2)}{p^f} \ll \sum_{B(r)<p\leq x^{1/f}} \frac{\log^2(p)}{p^{f/2}} \ll 1.$$

Therefore,

$$\frac{1}{|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t}\pi_E^{r,f}(x)=\begin{cases}\mathrm{O}\left(1+\frac{\log^2 x}{t}\right) & \text{for } f\geq 5\\ \mathrm{O}\left(1+\frac{\log\log x\log^2 x}{t}\right) & \text{for } f=4\\ \mathrm{O}\left(1+\frac{x^{1/6}\log x}{t}\right) & \text{for } f=3.\end{cases}$$

This concludes the proof of Theorem 3.0.17.

3.2 Counting Curves

Let $K/\mathbb{Q}$ be a Galois extension of degree n. Choose $\alpha_1,\ldots,\alpha_n$ so that $[\alpha_1,\ldots,\alpha_n]$ is a $\mathbb{Q}$-basis for K and $[\alpha_1,\ldots,\alpha_n]$ is an integral basis for $\mathcal{O}_K$. Let $p\in\mathbb{Z}$ be a rational prime, and $\mathfrak{p}_1,\ldots\mathfrak{p}_g$ be the distinct primes in $\mathcal{O}_K$ above p. Suppose that p does not ramify in $\mathcal{O}_K$, so that

$$p\mathcal{O}_K=\mathfrak{p}_1\cdots\mathfrak{p}_g.$$

Since K is Galois over $\mathbb{Q}$, there exist a positive integer f, so that $[\mathcal{O}_K/\mathfrak{p}_i:\mathbb{Z}/p\mathbb{Z}]=f$ for all i, $1\leq i\leq g$. The ring, $\mathcal{O}_K$ may be thought of as a $\mathbb{Z}$-module generated by α_i, $1\leq i\leq n$.

For a parameter $t\in\mathbb{R}$ to be chosen later recall the notation given in definition 3.0.15. For $\vec{v}\in\mathbb{Z}^n$ define

$$\|\vec{v}\|:=\max_{1\leq i\leq n}\{\vec{v}[i]\}$$

and

$$A'(\vec{v}):=\sum_{i=1}^{n}\vec{v}[i]\alpha_i.$$

Recall for $\vec{v_1},\vec{v_2}\in(\mathbb{Z}^n)^2$, we denote by $E_{\vec{v_1},\vec{v_2}}$ the elliptic curve

$$y^2=x^3+A'(\vec{v_1})x+A'(\vec{v_2}). \tag{3.2}$$

Recall the definition of $\mathcal{C}_t$

$$\mathcal{C}_t=\{E_{\vec{v_1},\vec{v_2}}:\|\vec{v_1}\|,\|\vec{v_2}\|\leq t\}.$$

Since

$$\begin{aligned}&\#\{(\vec{v},\vec{w}) \in (\mathbb{Z}^n)^2 \mid |\vec{v}[i]|, |\vec{w}[i]| \leq t \ ; \ 1 \leq i \leq n\}\\ &= (2t + \mathrm{O}(1))^{2n}\end{aligned}$$

we have

$$|\mathcal{C}_t| = 4^n t^{2n} + \mathrm{O}(t^{2n-1}).$$

Therefore,

$$\frac{1}{|\mathcal{C}_t|} = \frac{1}{4^n t^{2n}} + \mathrm{O}\left(\frac{1}{t^{2n+1}}\right). \tag{3.3}$$

Let $\mathfrak{p}$ be a prime in $\mathcal{O}_K$. The curve $E_{\vec{v_1},\vec{v_2}}$ from (3.2) is said to be *minimal* whenever the highest power of $\mathfrak{p}$ dividing the discriminant is minimized, that is whenever $\mathrm{ord}_{\mathfrak{p}}(\Delta(E_{\vec{v_1},\vec{v_2}}))$ is minimized. According to Silverman [32, pg. 172] if $\mathfrak{p} \nmid 6$, then $E_{\vec{v_1},\vec{v_2}}$ is minimal if and only if $\mathrm{ord}_{\mathfrak{p}}(A'(\vec{v_1})) < 4$ or $\mathrm{ord}_{\mathfrak{p}}(A'(\vec{v_2})) < 6$. Let $E_{A,B}$ be an elliptic curve defined over $\mathcal{O}_K/\mathfrak{p}$, and let $\mathcal{C}_t(E_{A,B})$ denote the set of elliptic curves $E \in \mathcal{C}_t$ which reduce to $E_{A,B}$ over $\mathcal{O}_K/\mathfrak{p}$. To reduce $E_{\vec{v_1},\vec{v_2}}$ modulo $\mathfrak{p}$ we mean that one should first obtain a model

$$E : y^2 = x^3 + u^4 A'(\vec{v_1}) + u^6 A'(\vec{v_2})$$

which is minimal at $\mathfrak{p}$, then reduce the coefficients of the minimal model (see [32, Chapter 7]). Denote by $E^{\mathfrak{p}}_{\vec{v_1},\vec{v_2}}$ the reduction of $E_{\vec{v_1},\vec{v_2}}$ modulo $\mathfrak{p}$. We find asymptotics for the size of the set $\mathcal{C}_t(E_{A,B})$ by thinking of $p^N\mathcal{O}_K$ and $\mathfrak{p}^N$ as $\mathbb{Z}$-modules, where $N \geq 1$. We start with the following inclusions,

$$p^N\mathcal{O}_K \subseteq \mathfrak{p}^N \subseteq \mathcal{O}_K.$$

Since $p^N\mathcal{O}_K$ and $\mathfrak{p}^N$ are $\mathbb{Z}$-submodules of $\mathcal{O}_K$ the third isomorphism theorem for modules gives

$$\frac{(\mathcal{O}_K)/(p^N\mathcal{O}_K)}{(\mathfrak{p}^N)/(p^N\mathcal{O}_K)} \cong \frac{\mathcal{O}_K}{\mathfrak{p}^N}$$

Therefore,

$$\left|\mathfrak{p}^N/p^N\mathcal{O}_K\right| = p^{N(n-f)}.$$

Set $s = p^{N(n-f)}$. Suppose $\{\rho_1, \dots \rho_s\}$ is a complete set of distinct coset representatives for $\mathfrak{p}^N/p^N\mathcal{O}_K$. Then for $A \in \mathfrak{p}^N$, and $\vec{v} \in \mathbb{Z}^n$ we have

$$\begin{aligned}
&A'(\vec{v}) \equiv A \pmod{\mathfrak{p}^N} \\
\Leftrightarrow\ &A'(\vec{v}) - A \in \mathfrak{p}^N \\
\Leftrightarrow\ &A'(\vec{v}) - A \equiv \rho_i \pmod{p^N\mathcal{O}_K} \quad (\text{some } 1 \le i \le s) \\
\Leftrightarrow\ &A'(\vec{v}) \equiv A + \rho_i \pmod{p^N\mathcal{O}_K} \quad (\text{some } 1 \le i \le s).
\end{aligned}$$

For $1 \le i \le s$ set

$$A + \rho_i = \sum_{j=1}^{n} c_{i,j}\alpha_j \qquad c_{i,j} \in \mathbb{Z}.$$

Then

$$\begin{aligned}
&\#\{\vec{v} \in \mathbb{Z}^n | A'(\vec{v}) \equiv A \pmod{\mathfrak{p}^N}; \|\vec{v}\| \le t\} \\
&= \sum_{i=1}^{s} \#\left\{(c_{i,1} + p^N k_1, c_{i,2} + p^N k_2, \dots, c_{i,n} + p^N k_n) \ : \ \begin{matrix} |c_{i,j} + p^N k_j| \le t; \\ 1 \le j \le n \end{matrix}\right\} \\
&= \sum_{i=1}^{s} \left(\frac{2t}{p^N} + \mathrm{O}(1)\right)^n \qquad (3.4) \\
&= p^{N(n-f)}\left[\left(\frac{2t}{p^N}\right)^n + \mathrm{O}\left(\frac{t^{n-1}}{p^{Nn-N}}\right)\right] \\
&= \frac{(2t)^n}{p^{Nf}} + \mathrm{O}\left(\frac{t^{n-1}}{p^{N(f-1)}}\right).
\end{aligned}$$

Therefore, for $A, B \in \mathcal{O}_K/\mathfrak{p}$,

$$\begin{aligned}
&\#\left\{(\vec{v_1}, \vec{v_2}) \in (\mathbb{Z}^n)^2 \ : \ \begin{matrix} A'(\vec{v_1}) \equiv A \pmod{\mathfrak{p}}; A'(\vec{v_2}) \equiv B \pmod{\mathfrak{p}}; \\ \|\vec{v_1}\|, \|\vec{v_2}\| \le t \end{matrix}\right\} \\
&= \left[\left(\frac{2^n t^n}{p^f}\right) + \mathrm{O}\left(\frac{t^{n-1}}{p^{f-1}}\right)\right]^2 \\
&= \left(\frac{2^n t^n}{p^f}\right)^2 + \mathrm{O}\left(\frac{t^{2n-1}}{p^{2f-1}}\right).
\end{aligned}$$

Considering non-minimal models we see that

$$\begin{aligned}
&|\ \mathcal{C}_t(E_{A,B})| \\
&= \#\left\{(\vec{v_1},\vec{v_2}) \in (\mathbb{Z}^n)^2 \mid E^{\mathfrak{p}}_{\vec{v_1},\vec{v_2}} = E_{A,B}\ \right\} \\
&= \#\left\{(\vec{v_1},\vec{v_2}) \in (\mathbb{Z}^n)^2\ : \begin{matrix} A'(\vec{v_1}) \equiv A \pmod{\mathfrak{p}}; A'(\vec{v_2}) \equiv B \pmod{\mathfrak{p}}; \\ \|\vec{v_1}\|, \|\vec{v_2}\| \leq t \end{matrix}\right\} \\
&\qquad + \mathrm{O}(\#\{\text{non-minimal models}\}) \\
&= \left(\frac{2^n t^n}{p^f}\right)^2 + \mathrm{O}\left(\frac{t^{2n-1}}{p^{2f-1}}\right) + \mathrm{O}(\#\{\text{non-minimal models}\})
\end{aligned}$$

Recall that if $\mathfrak{p} \nmid 6$, then $E_{\vec{v_1},\vec{v_2}}$ is minimal if and only if $\mathrm{ord}_{\mathfrak{p}}(A'(\vec{v_1})) < 4$ and $\mathrm{ord}_{\mathfrak{p}}(A'(\vec{v_2})) < 6$. Therefore, we estimate $\#\{\text{non - minimal models}\}$ as follows.

$$\#\{\text{non-minimal models}\} = \#\{E_{\vec{v_1},\vec{v_2}} \in \mathcal{C}_t : A'(\vec{v_1}) \in \mathfrak{p}^4 \text{ and } A'(\vec{v_2}) \in \mathfrak{p}^6\}.$$

Using the estimates from (3.4) we have

$$\left(\frac{(2t)^n}{p^4 f} + \mathrm{O}\left(\frac{t^{n-1}}{p^{4(f-1)}}\right)\right)\left(\frac{(2t)^n}{p^6 f} + \mathrm{O}\left(\frac{t^{n-1}}{p^{6(f-1)}}\right)\right).$$

Hence, accounting for non-minimal models we have

$$\begin{aligned}
|\mathcal{C}_t(E_{A,B})| &= \#\{E_{\vec{v_1},\vec{v_2}} \in \mathcal{C}_t | E^{\mathfrak{p}}_{\vec{v_1},\vec{v_2}} = E_{A,B}\} \\
&= \left(\frac{2^n t^n}{p^f}\right)^2 + \mathrm{O}\left(\frac{t^{2n-1}}{p^{2f-1}}\right) + \mathrm{O}\left(\frac{t^n}{p^4 f} \cdot \frac{t^n}{p^6 f}\right) \\
&= \left(\frac{(2t)^{2n}}{p^{2f}}\right) + \mathrm{O}\left(\frac{t^{2n-1}}{p^{2f-1}} + \frac{t^{2n}}{p^{10f}}\right)
\end{aligned}$$

3.3 The Average in Terms of L-Series

Before proving Lemma 3.0.19 we discuss the Kronecker class number and the Hurwitz class number. In [30] Schoof defines the Kronecker class number as follows. For $a, b, c \in \mathbb{Z}$ with $a > 0$ let $\Delta_f = b^2 - 4ac$ be the discriminant of the binary quadratic form

$f = ax^2 + bxy + cy^2$. For $\Delta < 0$, Schoof defines

$$K(\Delta) = \sum_{\substack{[f] \\ \Delta_f = \Delta}} 1$$

where the sum runs over classes of binary quadratic forms of discriminant Δ.

A definition of the Hurwitz class number used by Lenstra in [27] and the definition we use is as follows. For $\Delta > 0$, we define

$$H(\Delta) = \sum_{\substack{[f] \\ \Delta_f = -\Delta}} c_f$$

where

$$c_f = \begin{cases} \frac{1}{2} & \text{if } f \text{ is proportional to } x^2 + y^2, \\ \frac{1}{3} & \text{if } f \text{ is proportional to } x^2 + xy + y^2, \\ 1 & \text{otherwise.} \end{cases}$$

Since among forms of discriminant Δ there cannot be forms proportional to $x^2 + y^2$ and forms proportional to $x^2 + xy + y^2$, we cannot have both a 1/2 and a 1/3 show up in the sum above. Consider the form $f = ax^2 + bxy + cy^2$. f is proportional to $x^2 + y^2$[resp. $x^2 + xy + y^2$] means there exists $\alpha \in \mathbb{Z}$[resp. $\beta \in \mathbb{Z}$] such that $f = \alpha(x^2 + y^2)$[resp. $f = \beta(x^2 + xy + y^2)$]. The discriminants of these forms are $\Delta_f = b^2 - 4ac$, $\Delta_{\alpha(x^2+y^2)} = -4\alpha^2$, and $\Delta_{\beta(x^2+xy+y^2)} = -3\beta^2$. Since $4\alpha^2 \neq 3\beta^2$ for any $\alpha, \beta \in \mathbb{Z}$, the sum above has one summand which differs from one. Therefore, $H(\Delta) = K(\Delta) + \mathrm{O}(1)$. In [8] David and Pappalardi state the following well-known formula for the Hurwitz class number. Let $D > 0$ be the discriminant of a quadratic imaginary order then

$$H(D) = 2 \sum_{\substack{k^2 | D \\ \frac{D}{k^2} \equiv 0,1 \pmod 4}} \frac{h(D/k^2)}{w(D/k^2)},$$

where $h(d)$ and $w(d)$ denote respectively the Dirichlet class number and the number of units of the order of discriminant d. For $p > 3$ and $f \geq 1$ any elliptic curve over $\mathbb{F}_{p^f}$

may be written as

$$E_{a,b} : y^2 = x^3 + ax + b$$

with $a, b \in \mathbb{F}_{p^f}$. According to [27, Lenstra] the elliptic curves $E_{a',b'}$ over $\mathbb{F}_{p^f}$ which are $\mathbb{F}_{p^f}$-isomorphic to $E_{a,b}$ are given by all choices

$$a' = u^4 a \text{ and } b' = u^6 b$$

with $u \in \mathbb{F}_{p^f}^*$. The number of such $E_{a',b'}$ is

$$\begin{cases} \frac{p^f-1}{6} & \text{when } a = 0 \text{ and } p^f \equiv 1 \pmod 3 \\ \frac{p^f-1}{4} & \text{when } b = 0 \text{ and } p^f \equiv 1 \pmod 4 \\ \frac{p^f-1}{2} & \text{otherwise.} \end{cases}$$

Following Schoof [30] we define $N(r)$ to be the number of $\mathbb{F}_{p^f}$-isomorphism classes of elliptic curves with $p^f + 1 - r$ points defined over $\mathbb{F}_{p^f}$. Then by Deuring's Theorem (see [9] or [30, Theorem 4.6]) if $r^2 - 4p^f < 0$ and $p \nmid r$, then

$$N(r) = K(r^2 - 4p^f).$$

Therefore,

$$N(r) = H(4p^f - r^2) + \mathrm{O}(1).$$

Let $T_{p^f}(r)$ be the number of models over $\mathbb{F}_{p^f}$ of the form

$$E_{A,B} : y^2 = x^3 + Ax + B.$$

with $p^f + 1 - r$ rational points. Then using Deuring's theorem we have

Theorem 3.3.1.

$$T_{p^f}(r) = H(4p^f - r^2)\frac{p^f}{2} + \mathrm{O}(p^f).$$

Proof.

Let $\tilde{E}$ denote an $\mathbb{F}_{p^f}$-isomorphism class. Then

$$\begin{aligned} T_{p^f}(r) &= \sum_{\substack{\tilde{E}/\mathbb{F}_{p^f} \\ a_{\mathfrak{p}}(\tilde{E})=r}} \sum_{\substack{A,B \\ E_{A,B}\in\tilde{E}}} 1 \\ &= \sum_{\substack{\tilde{E}/\mathbb{F}_{p^f} \\ a_{\mathfrak{p}}(\tilde{E})=r \\ \#\{A,B:E_{A,B}\in\tilde{E}\}=\frac{p^f-1}{2}}} \frac{p^f-1}{2} + \mathrm{O}\left(\sum_{\substack{\tilde{E}/\mathbb{F}_{p^f} \\ a_{\mathfrak{p}}(\tilde{E})=r \\ \#\{A,B:E_{A,B}\in\tilde{E}\}\neq\frac{p^f-1}{2}}} p^f \right) \end{aligned}$$

Since there are at most 10 classes with size different from $\frac{p^f-1}{2}$ we have

$$\begin{aligned} T_{p^f}(r) &= \sum_{\substack{\tilde{E}/\mathbb{F}_{p^f} \\ a_{\mathfrak{p}}(\tilde{E})=r}} \frac{p^f-1}{2} + \mathrm{O}\left(p^f\right) \\ &= \frac{p^f-1}{2} H(4p^f - r^2) + \mathrm{O}(p^f). \end{aligned}$$

Using the class number formula

$$h(d) = \frac{w(d)|d|^{1/2}}{2\pi} L(1, \chi_d) \qquad \text{for } d < 0$$

along with $L(1, \chi_{\Delta_k}) \ll \log p$ (see [27, pg. 656]) and noting that r odd implies that $\frac{r^2-4p^f}{k^2} \equiv 1 \pmod 4$, we obtain

$$\begin{aligned} H(4p^f - r^2) &= 2 \sum_{k^2 | 4p^f - r^2} \frac{h((r^2-4p^f)/k^2)}{w((r^2-4p^f)/k^2)} \\ &= \frac{1}{\pi} \sum_{k^2 | 4p^f - r^2} \frac{\sqrt{4p^f - r^2}}{k} L(1, \chi_{(r^2-4p^f)/k^2}) \\ &\ll \sum_{k^2 | 4p^f - r^2} \frac{p^{f/2}}{k} \log p \\ &\ll p^{f/2} \log^2 p. \end{aligned}$$

The result follows.

□

Proof of Lemma 3.0.19.

We begin by writing $\pi_E^{r,f}(x)$ as a sum.

$$\frac{1}{|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t}\pi_E^{r,f}(x)=\frac{1}{|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t}\sum_{\substack{N(\mathfrak{p})\leq x\\ \deg_K\mathfrak{p}=f\\ a_{\mathfrak{p}}(E)=r}}1$$

Using $N(\mathfrak{p})=p^f$ we rewrite the inner sum as a sum on p. There are $g=n/f$ primes in $\mathcal{O}_K$ which lie above each rational prime p. Therefore

$$\frac{1}{|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t}\sum_{\substack{N(\mathfrak{p})\leq x\\ \deg_K\mathfrak{p}=f\\ a_{\mathfrak{p}}(E)=r}}1=\frac{n}{f|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t}\sum_{\substack{p^f\leq x\\ g(p)=n/f\\ a_{\mathfrak{p}}(E)=r}}1=\frac{n}{f|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t}\sum_{\substack{B(r)<p\leq x^{1/f}\\ g(p)=n/f\\ a_{\mathfrak{p}}(E)=r}}1+\mathrm{O}(1)$$

where $g(p)$ is the number of primes of $\mathcal{O}_K$ lying above p and the O-term comes from the finite number of primes removed from the inner sum. We set $B(r)=\max\{(r^2/4)^{1/f},r,3\}$ for several reasons. First, to ensure that $|r|\leq 2\sqrt{N(\mathfrak{p})}$, which is a necessary condition in Hasse's theorem. Secondly, we need $r<p$ to ensure that $p\nmid r$ (for Deuring's theorem). Recall that an elliptic curve defined over a field K has Weierstrass equation $y^2=x^3+ax+b$ if the characteristic of K is not 2 or 3. Hence, we require $p>3$.

Reversing summation we have

$$\begin{aligned}&\frac{n}{f|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t}\sum_{\substack{B(r)<p\leq x^{1/f}\\ g(p)=n/f\\ a_{\mathfrak{p}}(E)=r}}1+\mathrm{O}(1)\\ &=\frac{n}{f|\mathcal{C}_t|}\sum_{\substack{B(r)<p\leq x^{1/f}\\ g(p)=n/f}}\sum_{\substack{E\in\mathcal{C}_t\\ a_{\mathfrak{p}}(E)=r}}1+\mathrm{O}(1)\end{aligned}\tag{3.5}$$

Given a rational prime p let $\mathfrak{p}$ be any prime of $\mathcal{O}_K$ lying above p. Then the inner most sum of (3.5) becomes

$$\sum_{\substack{E\in\mathcal{C}_t\\ a_{\mathfrak{p}}(E)=r}} 1 = \sum_{\substack{E_{A,B}/\mathbb{F}_{p^f}\\ \#E_{A,B}(\mathbb{F}_{p^f})=p^f+1-r}} |\mathcal{C}_t(E_{A,B})| + \mathrm{O}\left(\sum_{\substack{E\in\mathcal{C}_t\\ E^{\mathfrak{p}}\text{ is}\\ \text{singular}}} 1\right)$$

We estimate the O-term as follows

$$\begin{aligned}\sum_{\substack{E\in\mathcal{C}_t\\ E^{\mathfrak{p}}\text{is}\\ \text{singular}}} 1 &= \sum_{A\in\mathcal{O}_K/\mathfrak{p}} \sum_{\substack{B\in\mathcal{O}_K/\mathfrak{p}\\ 4A^3-27B^2\in\mathfrak{p}}} |\mathcal{C}_t(E_{A,B})|\\ &\ll \sum_{A\in\mathcal{O}_K/\mathfrak{p}} \frac{(2t)^{2n}}{p^{2f}}\\ &\ll \frac{t^{2n}}{p^f}.\end{aligned}$$

Recall from the previous section that given $E/\mathbb{F}_{p^f}$,

$$|\mathcal{C}_t(E)| = \left(\frac{(2t)^{2n}}{p^{2f}}\right) + \mathrm{O}\left(\frac{t^{2n-1}}{p^{2f-1}} + \frac{t^{2n}}{p^{10f}}\right). \tag{3.6}$$

Therefore, the main term is

$$\sum_{\substack{E_{A,B}/\mathbb{F}_{p^f}\\ \#E_{A,B}(\mathbb{F}_{p^f})=p^f+1-r}} |\mathcal{C}_t(E_{A,B})| = T_{p^f}(r)\left[\left(\frac{(2t)^{2n}}{p^{2f}}\right) + \mathrm{O}\left(\frac{t^{2n-1}}{p^{2f-1}} + \frac{t^{2n}}{p^{10f}}\right)\right]$$

Applying Theorem 3.3.1 we have

$$\begin{aligned}\sum_{\substack{E\in\mathcal{C}_t\\ a_{\mathfrak{p}}(E)=r}} 1 &= T_{p^f}(r)\left[\left(\frac{(2t)^{2n}}{p^{2f}}\right) + \mathrm{O}\left(\frac{t^{2n-1}}{p^{2f-1}} + \frac{t^{2n}}{p^{10f}}\right)\right] + \mathrm{O}\left(\frac{t^{2n}}{p^f}\right)\\ &= \left(H(4p^f-r^2)\frac{p^f}{2} + \mathrm{O}(p^f)\right)\left(\left(\frac{(2t)^{2n}}{p^{2f}}\right) + \mathrm{O}\left(\frac{t^{2n-1}}{p^{2f-1}} + \frac{t^{2n}}{p^{10f}}\right)\right) + \mathrm{O}\left(\frac{t^{2n}}{p^f}\right)\end{aligned}$$

Recall (3.3)

$$\frac{1}{|\mathcal{C}_t|} = \left(\frac{1}{4^n t^{2n}} + \mathrm{O}\left(\frac{1}{t^{2n+1}}\right)\right)$$

then

$$\begin{aligned}
&\frac{1}{|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t}\pi_E^{r,f}(x)\\
&=\frac{n}{f}\left(\frac{1}{4^n t^{2n}}+\mathrm{O}\left(\frac{1}{t^{2n+1}}\right)\right)\sum_{\substack{B(r)<p\le x^{1/f}\\ g(p)=n/f}}\Bigg[\left(\left(\frac{(2t)^{2n}}{p^{2f}}\right)+\mathrm{O}\left(\frac{t^{2n-1}}{p^{2f-1}}+\frac{t^{2n}}{p^{10f}}\right)\right)\cdot\\
&\qquad\left(\frac{p^f}{2}H(4p^f-r^2)+\mathrm{O}(p^f)\right)+\mathrm{O}\left(\frac{t^{2n}}{p^f}\right)\Bigg]+\mathrm{O}(1)
\end{aligned}$$

Rearranging we may write

$$\begin{aligned}
&\frac{1}{|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t}\pi_E^{r,f}(x) \qquad (3.7)\\
&=\frac{n}{f}\sum_{\substack{B(r)<p\le x^{1/f}\\ g(p)=n/f}}\Bigg[\left(\frac{1}{4^n t^{2n}}+\mathrm{O}\left(\frac{1}{t^{2n+1}}\right)\right)\left(\left(\frac{(2t)^{2n}}{p^{2f}}\right)+\mathrm{O}\left(\frac{t^{2n-1}}{p^{2f-1}}+\frac{t^{2n}}{p^{10f}}\right)\right)\cdot\\
&\qquad\left(\frac{p^f}{2}H(4p^f-r^2)+\mathrm{O}(p^f)\right)\Bigg]+\mathrm{O}\left(\sum_{\substack{B(r)<p\le x^{1/f}\\ g(p)=n/f}}\frac{1}{p^f}\right)+\mathrm{O}(1)
\end{aligned}$$

Recall $H(4p^f-r^2)\ll p^{f/2}\log^2 p$ (see 75). Therefore, the expression within the brackets in (3.7) becomes

$$\begin{aligned}
&\left(\frac{1}{4^n t^{2n}}+\mathrm{O}\left(\frac{1}{t^{2n+1}}\right)\right)\left(\left(\frac{(2t)^{2n}}{p^{2f}}\right)+\mathrm{O}\left(\frac{t^{2n-1}}{p^{2f-1}}+\frac{t^{2n}}{p^{10f}}\right)\right)\\
&\qquad\cdot\left(\frac{p^f}{2}H(4p^f-r^2)+\mathrm{O}(p^f)\right)\\
&=\frac{H(4p^f-r^2)}{2p^f}\\
&+\mathrm{O}\left(\frac{1}{p^f}+\frac{p^f H(4p^f-r^2)}{t^{2n}}\left(\frac{t^{2n-1}}{p^{2f-1}}+\frac{t^{2n}}{p^{10f}}\right)+\frac{t^{2n}H(4p^f-r^2)}{p^f t^{2n+1}}\right)\\
&=\frac{H(4p^f-r^2)}{2p^f}+\mathrm{O}\left(\frac{1}{p^f}+\frac{\log^2 p}{p^{17f/2}}+\log^2 p\left(\frac{1}{tp^{f/2-1}}+\frac{1}{p^{f/2}t}\right)\right)\\
&=\frac{H(4p^f-r^2)}{2p^f}+\mathrm{O}\left(\frac{1}{p^f}+\frac{\log^2 p}{tp^{f/2-1}}\right)
\end{aligned}$$

Substituting into (3.7) we have

$$\begin{aligned}&\frac{1}{|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t}\pi_E^{r,f}(x)\\&=\frac{n}{f}\sum_{\substack{B(r)<p\le x^{1/f}\\ g(p)=n/f}}\left[\frac{H(4p^f-r^2)}{2p^f}+\mathrm{O}\left(\frac{1}{p^f}+\frac{\log^2 p}{tp^{f/2-1}}\right)\right].\end{aligned}$$

Write

$$\frac{1}{|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t}\pi_E^{r,f}(x)=\frac{n}{2f}\sum_{\substack{B(r)<p\le x^{1/f}\\ g(p)=n/f}}\frac{H(4p^f-r^2)}{p^f}+E(x,t). \tag{3.8}$$

First we deal with the O-term in (3.8). For $f=1$ we use the estimates

$$\begin{aligned}\sum_{p<x}\frac{1}{p}&\ll\log\log x,\\\sum_{p<x}\frac{\sqrt{p}\log^2 p}{t}&\ll\frac{x}{t\log x}\sqrt{x}\log^2 x=\frac{x^{3/2}\log x}{t}.\end{aligned}$$

For $f=2$ we use

$$\sum_{p<\sqrt{x}}\frac{\log^2 p}{t}\ll\frac{\sqrt{x}}{\log\sqrt{x}}\frac{\log^2\sqrt{x}}{t}\ll\frac{\sqrt{x}\log x}{t}.$$

For $f=3$ we recall the partial summation formula. Let $\{a_n\}$ be a sequence of complex numbers. Set

$$A(y)=\sum_{n\le y}a_n\qquad(y>0).$$

Let $f(y)$ be a continously differentiable function on the interval $[m,X]$. Then we have

$$\sum_{m\le n\le X}a_nf(n)=A(X)f(X)-\int_1^X A(y)f'(y)\ \mathrm{dy}-A(m-1)f(m)$$

where $A(-1)=0$. A proof of the partial summation formula follows directly from Murty's proof found in [29, Theorem 2.2].

Suppose $f = 3$. Set $f(y) = y^{-1/2}$ and set

$$a_n = \begin{cases} \log^2 n & \text{if } n \text{ is prime,} \\ 0 & \text{otherwise.} \end{cases}$$

Then partial summation gives

$$\sum_{p<x^{1/3}} \frac{\log^2 p}{tp^{1/2}} \ll \frac{x^{1/6}\log x}{t}.$$

Suppose $f = 4$. Then using $\sum_{p<x} \frac{1}{p} \ll \log\log x$ we have

$$\sum_{p<x^{1/4}} \frac{\log^2 p}{tp} \ll \frac{\log^2 x}{t} \sum_{p<x} \frac{1}{p} \ll \frac{\log^2 x \log\log x}{t}.$$

For $f \geq 5$ use

$$\sum_{p<x^{1/f}} \frac{\log^2 p}{tp^{f/2-1}} \ll \frac{\log^2 x}{t} \sum_{p<x^{1/f}} \frac{1}{p^{3/2}} \ll \frac{\log^2 x}{t} \sum_{n=1}^{x^{1/f}} \frac{1}{n^{3/2}} \ll \frac{\log^2 x}{t}$$

Therefore, we have

$$E(x,t) \ll \begin{cases} 1 + \frac{\log^2 x}{t} & \text{for } f \geq 5 \\ 1 + \frac{\log^2 x \log\log x}{t} & \text{for } f = 4 \\ 1 + \frac{x^{1/6}\log x}{t} & \text{for } f = 3 \\ 1 + \frac{\sqrt{x}\log x}{t} & \text{for } f = 2 \\ \log\log x + \frac{x^{3/2}\log x}{t} & \text{for } f = 1. \end{cases} \tag{3.9}$$

Now we deal with the main term in (3.8). Let $d_k(p) = \frac{r^2-4p^f}{k^2}$. From the formula for the Hurwitz class number

$$H(4p^f - r^2) = \sum_{k^2|4p^f-r^2} \frac{h(d_k(p))}{w(d_k(p))}$$

and by the class number formula

$$h(d_k(p)) = \frac{w(d_k(p))|d_k(p)|^{1/2}}{2\pi} L(1, \chi_{d_k(p)})$$

we have

$$\frac{n}{2f}\sum_{B(r)<p\le x^{1/f}}\frac{H(4p^f-r^2)}{p^f}=\frac{n}{2\pi f}\sum_{\substack{B(r)<p\le x^{1/f}\\ g(p)=n/f}}\sum_{k^2|r^2-4p^f}\frac{\sqrt{4p^f-r^2}}{kp^f}L(1,\chi_{d_k(p)}).$$

Switching the order of summation and noticing that we need only consider $k\le 2x^{f/2}$, we have

$$\frac{n}{2\pi f}\sum_{\substack{B(r)<p\le x^{1/f}\\ g(p)=n/f}}\sum_{k^2|r^2-4p^f}\frac{\sqrt{4p^f-r^2}}{kp^f}L(1,\chi_{d_k(p)})$$
$$=\frac{n}{2\pi f}\sum_{k\le 2x^{f/2}}\frac{1}{k}\sum_{\substack{B(r)<p\le x^{1/f}\\ k^2|r^2-4p^f\\ g(p)=n/f}}\frac{\sqrt{4p^f-r^2}}{p^f}L(1,\chi_{d_k(p)}).$$

Approximate $\sqrt{4p^f-r^2}$ by $2\sqrt{p^f}+\mathrm{O}\left(\frac{1}{p^{f/2}}\right)$ and use the fact that $L(1,\chi_{d_k(p)})\ll\log p$ (see [27, pg. 656]) to obtain

$$\frac{n}{\pi f}\sum_{k\le 2x^{f/2}}\frac{1}{k}\left[\sum_{\substack{B(r)<p\le x^{1/f}\\ k^2|r^2-4p^f\\ g(p)=n/f}}\frac{L(1,\chi_{d_k(p)})}{p^{f/2}}+\mathrm{O}\left(\sum_{\substack{B(r)<p\le x^{1/f}\\ k^2|r^2-4p^f\\ g(p)=n/f}}\frac{\log p}{p^{3f/2}}\right)\right] \tag{3.10}$$

for the O-term we use the fact that for any integer m

$$\sum_{k|m}1\ll m^{\epsilon}\qquad\text{for all }\epsilon>0$$

(see [29, Exercise 1.3.2]) to see that

$$\sum_{k\le 2x^{f/2}}\frac{1}{k}\sum_{\substack{B(r)<p\le x^{1/f}\\ k^2|r^2-4p^f\\ g(p)=n/f}}\frac{\log p}{p^{3f/2}}\ll\sum_{p\le x^{1/f}}\left(\sum_{k^2|r^2-4p^f}\frac{1}{k}\right)\frac{\log p}{p^{3f/2}}\ll\sum_{p\le x^{1/f}}\frac{p^{\epsilon}\log p}{p^{3f/2}}\ll 1$$

Set $f(y) = (y^{f/2}\log y)^{-1}$ and set

$$a_n = \begin{cases} L(1,\chi_{d_k(p)})\log p & \text{if } n \text{ is prime and } n > B(r), \\ 0 & \text{otherwise.} \end{cases}$$

Using partial summation (see pg. 79) the main term in (3.10) becomes

$$\begin{aligned} &\frac{n}{\pi f}\sum_{k\le 2x^{f/2}}\frac{1}{k}\sum_{\substack{B(r)<p\le x^{1/f}\\ k^2|r^2-4p^f\\ g(p)=n/f}}\frac{L(1,\chi_{d_k(p)})}{p^{f/2}} \\ &= \frac{n}{\pi f\sqrt{x}\log x^{1/f}}\sum_{k\le 2x^{f/2}}\frac{1}{k}\sum_{\substack{B(r)<p\le x^{1/f}\\ k^2|r^2-4p^f\\ g(p)=n/f}}L(1,\chi_{d_k(p)})\log p \\ &\quad -\frac{n}{\pi f}\int_{B(r)}^{x^{1/f}}\sum_{k\le 2x^{f/2}}\frac{1}{k}\sum_{B(r)<p\le s}L(1,\chi_{d_k(p)})\log p\frac{\mathrm{d}}{\mathrm{ds}}\left(\frac{1}{s^{f/2}\log s}\right)\,\mathrm{ds}. \end{aligned}$$

Set $s = S^{1/f}$ and note that $k^2|4p^f - r^2$ implies $k < 2S^{f/2}$ to obtain

$$\begin{aligned} &\frac{n}{\pi f}\sum_{k\le 2x^{f/2}}\frac{1}{k}\sum_{\substack{B(r)<p\le x^{1/f}\\ k^2|r^2-4p^f\\ g(p)=n/f}}\frac{L(1,\chi_{d_k(p)})}{p^{f/2}} \\ &= \frac{n}{\pi\sqrt{x}\log x}\sum_{k\le 2x^{f/2}}\frac{1}{k}\sum_{\substack{B(r)<p\le x^{1/f}\\ k^2|r^2-4p^f\\ g(p)=n/f}}L(1,\chi_{d_k(p)})\log p \\ &\quad -\frac{n}{\pi}\int_{B(r)^f}^{x}\sum_{k\le 2S^{f/2}}\frac{1}{k}\sum_{\substack{B(r)<p\le S^{1/f}\\ k^2|r^2-4p^f\\ g(p)=n/f}}L(1,\chi_{d_k(p)})\log p\frac{\mathrm{d}}{\mathrm{dS}}\left(\frac{1}{S^{1/2}\log S}\right)\,\mathrm{dS} \end{aligned}$$

since

$$\frac{\mathrm{d}}{\mathrm{dS}}\left(\frac{f}{S^{1/2}\log S}\right)\,\mathrm{dS} = \frac{\mathrm{d}}{\mathrm{ds}}\left(\frac{1}{s^{f/2}\log s}\right)\,\mathrm{ds}.$$

Therefore,

$$\begin{aligned}
&\frac{1}{|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t}\pi_E^{r,f}(x)\\
&=\frac{n}{\pi}\Bigg[\frac{1}{\sqrt{x}\log x}\sum_{k\leq 2x^{f/2}}\frac{1}{k}\sum_{\substack{B(r)<p\leq x^{1/f}\\ k^2|r^2-4p^f\\ g(p)=n/f}}L(1,\chi_{d_k(p)})\log p\\
&\quad-\int_{B(r)^f}\sum_{k\leq 2S^{f/2}}\frac{1}{k}\sum_{\substack{B(r)<p\leq S^{1/f}\\ k^2|r^2-4p^f\\ g(p)=n/f}}L(1,\chi_{d_k(p)})\log p\frac{\mathrm{d}}{\mathrm{dS}}\left(\frac{1}{S^{1/2}\log S}\right)\,\mathrm{ds}\Bigg]+E(x,t)
\end{aligned}$$

□

3.4 Computing $C_r(a,n,k)$

Recall that in the statement of Lemma 3.0.20 (1) we defined

$$C_{r,A,B}=\sum_{\substack{k\in\mathbb{N}\\(k,2r)=1}}\frac{1}{k}\sum_{n=1}^{\infty}\frac{1}{n\phi(4nBk^2)}\sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*}\left(\frac{a}{n}\right)C_r(a,n,k)$$

where

$$C_r(a,n,k)=$$
$$\#\{b\in(\mathbb{Z}/4Bnk^2\mathbb{Z})^*:b\equiv A\pmod{B};4b^2\equiv r^2-ak^2\pmod{4nk^2}\}.$$

In section 3.5 we require an upper bound on

$$\sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*}\left(\frac{a}{n}\right)C_r(a,n,k)$$

in order to prove Lemma 3.0.20. In this section we provide a formula for $C_r(a,n,k)$ which will provide the requisite upper bound. The lemma proved in this section will also enable us to construct a multiplicative function in section 3.6 which will in turn allow us to prove a product formula for $C_{r,A,B}$ in section 3.7. For the main result in this section we require the following lemma.

Lemma 3.4.1. *Suppose A is odd, $2 \leq L \in \mathbb{Z}$, and $1 \leq k \in \mathbb{Z}$. Then for any $X \in \mathbb{Z}$,*

$$X \equiv MA + M^2 2^k \pmod{2^L}$$

has a unique solution M modulo 2^L.

Proof. It is easy to check the $L = 2$ case. We proceed by induction on L. To that end assume $X = MA + M^2 2^k \pmod{2^{L-1}}$ has a unique solution $M_0 \pmod{2^{L-1}}$ for $L \geq 3$. Given $A \equiv 1 \pmod 2$ and $1 \leq k \leq L-1$ ($k \geq L$ is obvious) consider $X \equiv MA + M^2 2^k \pmod{2^L}$. By our assumption there exists a unique M such that $X = MA + M^2 2^k \pmod{2^{L-1}}$, say $M = M_0$. We write $X - M_0 A - M_0^2 2^k = 2^{L-1} N$ for some $N \in \mathbb{Z}$. Set $M_1 = M_0 + 2^{L-1} Q$, where $Q \in \mathbb{Z}$. Then

$$\begin{aligned}
&X \equiv M_1 A + 2^k M_1^2 \pmod{2^L} \\
\Leftrightarrow\ & 2^{L-1} N = X - M_0 A - 2^k M_0^2 \equiv 2^{L-1}[AQ + QM_0 2^{k+1} + Q^2 2^{k+L-1}] \pmod{2^L} \\
\Leftrightarrow\ & N \equiv AQ + QM_0 2^{k+1} + Q^2 2^{k+L-1} \pmod 2 \\
\Leftrightarrow\ & N \equiv AQ + QM_0 2^{k+1} \pmod 2 \\
\Leftrightarrow\ & N \equiv Q \pmod 2
\end{aligned}$$

Therefore, choosing $Q \equiv N \pmod 2$ M_1 is the unique solution to $X \equiv MA + M^2 2^k \pmod{2^L}$ □

Let $p \in \mathbb{Z}$ be any prime. In order to compute $C_r(a, n, k)$, we note that by the Chinese Remainder Theorem

$$C_r(a, n, k) = \prod_{\substack{p \mid (4Bnk^2) \\ p \text{ prime}}} d_p(n)$$

where

$$d_p(n) = \sum_{\substack{b \in (\mathbb{Z}/p^l\mathbb{Z})^* \\ b \equiv A \pmod{p^{l_1}} \\ 4b^2 \equiv r^2 - ak^2 \pmod{p^{l_2}}}} 1$$

with $l = \mathrm{ord}_p(4Bnk^2),\ l_1 = \mathrm{ord}_p(B),\ l_2 = \mathrm{ord}_p(4nk^2)$.

Note that $l = l_1 + l_2$ and $ord_2(4nk^2) \geq 2$.

Lemma 3.4.2. *Let p be an odd prime. Using the notation above we have*

1. *Suppose $0 \leq l_2 \leq l_1$ and $l_1 > 0$. Then*

$$d_p(n) = \begin{cases} p^{l-l_1} & \text{if } 4A^2 \equiv r^2 - ak^2 \pmod{p^{l_2}} \\ 0 & \text{otherwise} \end{cases}$$

2. *Suppose $l_1 = 0$. Then*

$$d_p(n) = \begin{cases} 1 + \left(\frac{r^2-ak^2}{p}\right) & \text{if } (r^2 - ak^2, p) = 1 \\ 0 & \text{otherwise} \end{cases}$$

3. *Suppose $1 \leq l_1 < l_2$. Then*

$$d_p(n) = \begin{cases} p^{l-l_2} & \text{if } 4A^2 \equiv r^2 - ak^2 \pmod{p^{l_1}} \\ 0 & \text{otherwise} \end{cases}$$

4. *Suppose $l_1 = 0$ or $l_1 = 1$. Then*

$$d_2(n) = \begin{cases} 2^{\min(l_1+4, l-1)} & \text{if } r^2 - ak^2 \equiv 4 \pmod{2^{\min(5,l_2)}} \\ 0 & \text{if } r^2 - ak^2 \not\equiv 4 \pmod{2^{\min(5,l_2)}} \end{cases}$$

5. *If $l_1 \geq 2$ and $2 \leq l_2 \leq l_1 + 3$, then*

$$d_2(n) = \begin{cases} 2^{l-l_1} & \text{if } 4A^2 \equiv r^2 - ak^2 \pmod{2^{l-l_1}} \\ 0 & \text{if } 4A^2 \not\equiv r^2 - ak^2 \pmod{2^{l-l_1}} \end{cases}$$

6. *If $l_1 \geq 2$ and $l_2 \geq l_1 + 4$, then*

$$d_2(n) = \begin{cases} 2^{l_1+3} & \text{if } 4A^2 \equiv r^2 - ak^2 \pmod{2^{l_1+3}} \\ 0 & \text{if } 4A^2 \not\equiv r^2 - ak^2 \pmod{2^{l_1+3}} \end{cases}$$

Proof.

(1) It is easy to see that if $l_2 = 0$ and $l_1 > 0$, then $d_p(n) = 1$. So suppose $0 < l_2 \leq l_1$ and p is any odd prime. Then

$$\begin{aligned} & b \equiv A \pmod{p^{l_1}} \text{ and } 4b^2 \equiv r^2 - ak^2 \pmod{p^{l_2}} \\ & \Leftrightarrow \exists M \text{ such that } 4(A + Mp^{l_1})^2 \equiv r^2 - ak^2 \pmod{p^{l_2}} \\ & \Leftrightarrow 4(A^2 + 2MAp^{l_1} + M^2p^{2l_1}) \equiv r^2 - ak^2 \pmod{p^{l_2}} \\ & \Leftrightarrow 4A^2 \equiv r^2 - ak^2 \pmod{p^{l_2}}. \end{aligned}$$

Since $\#\{b \in (\mathbb{Z}/p^l\mathbb{Z})^* : b \equiv A \pmod{p^{l_1}}\} = p^{l-l_1}$, the result follows.

(2) If $l_1 = 0$, then $d_p(n)$ becomes

$$d_p(n) = \sum_{\substack{b \in (\mathbb{Z}/p^l\mathbb{Z})^* \\ 4b^2 \equiv r^2 - ak^2 \pmod{p^l}}} 1.$$

If $p|(r^2 - ak^2)$, then there are no solutions in $(\mathbb{Z}/p^l\mathbb{Z})^*$ to $4b^2 \equiv r^2 - ak^2 \pmod{p}$. If $(r^2 - ak^2, p) = 1$, then there are two or zero solutions to $4b^2 \equiv r^2 - ak^2 \pmod{p^l}$. If $r^2 - ak^2$ is a square modulo p then there are two solutions modulo p which lift to two solutions modulo p^l. On the other hand, if $r^2 - ak^2$ is not a square modulo p, then there are no solutions modulo p, hence there are no solutions modulo p^l.

(3) Suppose $l_2 > l_1 \geq 1$ and p is odd. If $b = A$ is a solution to $4b^2 \equiv r^2 - ak^2 \pmod{p^{l_1}}$, then $b \equiv A \pmod{p^{l_1}}$ lifts uniquely to a solution modulo p^{l_2}. Since $\#\{b \in (\mathbb{Z}/p^l\mathbb{Z})^* : b \equiv A \pmod{p^{l_2}}\} = p^{l-l_2}$, the result follows.

(4) Suppose $l_1 = 0$. Then

$$d_2(n) = \sum_{\substack{b \in (\mathbb{Z}/2^{l_2})^* \\ 4b^2 \equiv r^2 - ak^2 \pmod{2^{l_2}}}} 1.$$

The cases $l_2 = 2, 3$ and 4 may be checked directly. For $l_2 \geq 5$ the number of solutions to $b^2 \equiv \frac{r^2-ak^2}{4} \pmod{2^{l_2-2}}$ are 4 if $\frac{r^2-ak^2}{4} \equiv 1 \pmod{8}$ and 0 otherwise (see [18, pg. 98]). These four solutions lift to 16 solutions modulo 2^{l_2}.

Suppose $l_1 = 1$. Since B is even and $(A, B) = 1$ we see that A is odd. Thus,

$$d_p(n) = \sum_{\substack{b \in (\mathbb{Z}/2^{l_2+1})^* \\ 4b^2 \equiv r^2 - ak^2 \pmod{2^{l_2}}}} 1.$$

The cases $l_2 = 2, 3$ and 4 may be checked directly. For $l_2 \geq 5$ the number of solutions to $b^2 \equiv \frac{r^2-ak^2}{4} \pmod{2^{l_2-2}}$ are 4 if $\frac{r^2-ak^2}{4} \equiv 1 \pmod{8}$ and 0 otherwise (see [18, pg. 98]). These four solutions lift to 32 solutions modulo 2^{l_2+1}.

(5) Suppose $l_1 \geq 2$ and $2 \leq l_2 \leq l_1 + 3$. Observe

$$\begin{aligned}
&\exists\ b \quad \text{such that} \quad \begin{cases} b \equiv A \pmod{2^{l_1}} \\ 4b^2 \equiv r^2 - ak^2 \pmod{2^{l_2}} \end{cases} \\
&\Leftrightarrow \exists\ M \quad \text{such that} \quad 4(A + M2^{l_1})^2 \equiv r^2 - ak^2 \pmod{2^{l_2}} \\
&\Leftrightarrow 4(A^2 + 2^{l_1+1}MA + M^2 2^{2l_1}) \equiv r^2 - ak^2 \pmod{2^{l_2}} \\
&\Leftrightarrow 4A^2 + 2^{l_1+3}MA + M^2 2^{2l_1+2} \equiv r^2 - ak^2 \pmod{2^{l_2}} \\
&\Leftrightarrow 4A^2 \equiv r^2 - ak^2 \pmod{2^{l_2}}.
\end{aligned}$$

The result follows from the fact that there are 2^{l-l_1} $b \in (\mathbb{Z}/p^l\mathbb{Z})^*$ such that $b \equiv A \pmod{2^{l_1}}$.

(6) We consider three cases.

Case 1: Suppose $l_1 \geq 2$ and $l_2 = l_1 + 4$. Then

$$\begin{aligned}
&\exists\ b \quad \text{such that} \quad \begin{cases} b \equiv A \pmod{2^{l_1}} \\ 4b^2 \equiv r^2 - ak^2 \pmod{2^{l_2}} \end{cases} \\
&\Leftrightarrow \exists\ M \quad \text{such that} \quad (A + M2^{l_1})^2 \equiv \frac{r^2 - ak^2}{4} \pmod{2^{l_2-2}} \ \text{ and } \ \frac{r^2 - ak^2}{4} \in \mathbb{Z} \\
&\Leftrightarrow A^2 + 2^{l_1+1}MA + M^2 2^{2l_1} \equiv \frac{r^2 - ak^2}{4} \pmod{2^{l_1+2}} \ \text{ and } \ \frac{r^2 - ak^2}{4} \in \mathbb{Z} \\
&\Leftrightarrow \frac{r^2 - ak^2}{4} - A^2 \equiv 2^{l_1+1}MA + M^2 2^{2l_1} \pmod{2^{l_1+2}} \ \text{ and } \ \frac{r^2 - ak^2}{4} \in \mathbb{Z} \\
&\Leftrightarrow \frac{1}{2^{l_1+1}} \left[\frac{r^2 - ak^2}{4} - A^2 \right] \equiv MA + M^2 2^{l_1-1} \pmod{2} \ \text{ and } \ 2^{l_1+1} \Big| \left(\frac{r^2 - ak^2}{4} - A^2 \right) \\
&\Leftrightarrow \left(\frac{\frac{r^2-ak^2}{4} - A^2}{2^{l_1+1}} \right) \equiv M \pmod{2}
\end{aligned}$$

We require

$$\left(\frac{\frac{r^2-ak^2}{4} - A^2}{2^{l_1+1}} \right)$$

to be an integer. This requirement may be written as $4A^2 \equiv r^2 - ak^2 \pmod{2^{l_1+3}}$. Under this condition we have a unique M modulo 2 which gives a solution b modulo

2^{l_1+2}. Note if b satisfies $4b^2 \equiv r^2 - ak^2 \pmod{2^{l_2}}$, then so do $-b$, $b+2^{l_1+1}$, and $-b+2^{l_1+1}$. But only two of these four satisfy $b \equiv A \pmod{2^{l_1}}$. Therefore, the number of solutions is $2 \cdot 2^{l-(l_1+2)}$.

Case 2: Suppose $l_1 \geq 2$ and $l_2 = l_1 + 5$. Then

$$\exists\, b \quad \text{such that} \quad \begin{cases} b \equiv A \pmod{2^{l_1}} \\ 4b^2 \equiv r^2 - ak^2 \pmod{2^{l_2}} \end{cases}$$

$$\Leftrightarrow \exists\, M \quad \text{such that} \quad (A + M2^{l_1})^2 \equiv \frac{r^2 - ak^2}{4} \pmod{2^{l_2-2}} \text{ and } \frac{r^2 - ak^2}{4} \in \mathbb{Z}$$

$$\Leftrightarrow A^2 + 2^{l_1+1}MA + M^2 2^{2l_1} \equiv \frac{r^2 - ak^2}{4} \pmod{2^{l_1+3}} \text{ and } \frac{r^2 - ak^2}{4} \in \mathbb{Z}$$

$$\Leftrightarrow \frac{r^2 - ak^2}{4} - A^2 \equiv 2^{l_1+1}MA + M^2 2^{2l_1} \pmod{2^{l_1+3}} \text{ and } \frac{r^2 - ak^2}{4} \in \mathbb{Z}$$

$$\Leftrightarrow \frac{1}{2^{l_1+1}}\left[\frac{r^2 - ak^2}{4} - A^2\right] \equiv MA + M^2 2^{l_1-1} \pmod{4} \text{ and } 2^{l_1+1} \Big| \left(\frac{r^2 - ak^2}{4} - A^2\right)$$

$$\Leftrightarrow \left(\frac{\frac{r^2-ak^2}{4} - A^2}{2^{l_1+1}}\right) \equiv_4 \begin{cases} AM & \text{if } l_1 \geq 3 \\ AM + 2M^2 & \text{if } l_1 = 2 \end{cases}$$

We require $r^2 - ak^2 \equiv 4A^2 \pmod{2^{l_1+3}}$ so that the left hand side of the above equation is an integer. If $l_1 = 2$ we use Lemma 3.4.1 and see that we can find a *unique* M modulo 4 which satisfies

$$\left(\frac{\frac{r^2-ak^2}{4} - A^2}{2^{l_1+1}}\right) \equiv AM + 2M^2 \pmod{4}$$

which gives a unique b modulo 2^5. Note if b satisfies $b \equiv A \pmod{2^2}$ and $4b^2 \equiv r^2 - ak^2 \pmod{2^7}$, then so does $b + 2^4$. Therefore the number of solutions is $2 \cdot 2^{9-5} = 32$

If $l_1 \geq 3$, then it is easy to see that we have a unique M modulo 4 such that to

$$\left(\frac{\frac{r^2-ak^2}{4} - A^2}{2^{l_1+1}}\right) \equiv AM \pmod{4}.$$

which gives a unique b modulo 2^{l_1+3}. Note that if b satisfies $4b^2 \equiv r^2 - ak^2 \pmod{2^{l_1+5}}$, then so do $-b$, $b+2^{l_1+2}$, and $-b+2^{l_1+2}$. But, only two of these satisfy $b \equiv A \pmod{2^{l_1}}$. Thus, the number of solutions is $2 \cdot 2^{l-(l_1+3)} = 2^{l_1+3}$.

Case 3: Suppose $l_1 \geq 2$ and $l_2 \geq l_1 + 6$. Then

$$\begin{aligned}
&\exists\ b \quad \text{such that} \quad \begin{cases} b \equiv A \pmod{2^{l_1}} \\ 4b^2 \equiv r^2 - ak^2 \pmod{2^{l_2}} \end{cases} \\
&\Leftrightarrow \exists\ M \quad \text{such that} \quad (A + M2^{l_1})^2 \equiv \frac{r^2 - ak^2}{4} \pmod{2^{l_2-2}} \ \text{ and } \ \frac{r^2 - ak^2}{4} \in \mathbb{Z} \\
&\Leftrightarrow A^2 + 2^{l_1+1}MA + M^2 2^{2l_1} \equiv \frac{r^2 - ak^2}{4} \pmod{2^{l_2-2}} \ \text{ and } \ \frac{r^2 - ak^2}{4} \in \mathbb{Z} \\
&\Leftrightarrow \frac{r^2 - ak^2}{4} - A^2 \equiv 2^{l_1+1}MA + M^2 2^{2l_1} \pmod{2^{l_2-2}} \ \text{ and } \ \frac{r^2 - ak^2}{4} \in \mathbb{Z} \\
&\Leftrightarrow \left(\frac{\frac{r^2-ak^2}{4} - A^2}{2^{l_1+1}} \right) \equiv MA + M^2 2^{l_1-1} \pmod{2^{l_2-l_1-3}} \ \text{ and } \ 2^{l_1+1} \Big| \left(\frac{r^2 - ak^2}{4} - A^2 \right).
\end{aligned} \tag{3.11}$$

In order for the left hand side of (3.11) to be an integer, we must have

$$r^2 - ak^2 \equiv 4A^2 \pmod{2^{l_1+3}}. \tag{3.12}$$

By Lemma 3.4.1, (3.12) is a sufficient condition for determining a unique solution M modulo $2^{l_2-l_1-3}$ for (3.11). Then we obtain a solution b modulo 2^{l_2-2}. Note that if b satisfies $4b^2 \equiv r^2 - ak^2 \pmod{2^{l_2}}$, then so do $-b$, $b + 2^{l_2-3}$, and $-b + 2^{l_2-3}$. But, only two of these satisfy $b \equiv A \pmod{2^{l_1}}$. Thus, the number of solutions is $2^{l-l_2+2} \cdot 2$

□

3.5 Averaging Special Values of L-Series

In this section we prove Lemma 3.0.20 (2). For a proof of Lemma 3.0.20 (1) see [23, Proposition 2.1]. In [8] David and Pappalardi present a proof of Lemma 3.0.20 for $A = 3$ and $B = 4$. We let A and B be any coprime positive integers and consider primes up to $\sqrt{x}$. In the proof that follows we use arguments similar to those of David and Pappalardi (see [8, proof of Lemma 2.2]).

Proof of Lemma 3.0.20 (1).

Throughout this section we will be concerned with the double sum

$$\sum_{\substack{k\leq 2x\\(k,2r)=1}}\frac{1}{k}\sum_{\substack{B(r)<p\leq\sqrt{x}\\p\equiv A \pmod B\\4p^2\equiv r^2 \pmod{k^2}}} L(1,\chi_{d_k(p)})\log p.$$

Let U be a parameter to be determined. We have the following identity (see [8, (4.2)])

$$L(1,\chi_{d_k(p)}) := \sum_{n\in\mathbb{N}}\left(\frac{d_k(p)}{n}\right)\frac{1}{n} = \sum_{n\in\mathbb{N}}\left(\frac{d_k(p)}{n}\right)\frac{e^{-n/U}}{n} + \mathrm{O}\left(\frac{|d_k(p)|^{7/32}}{U^{1/2}}\right). \tag{3.13}$$

Before using the identity above we make two observations:

1. Since $d_k(p) = \frac{r^2-4p^2}{k^2}$,

$$|d_k(p)|^{7/32} \ll \left(\frac{p}{k}\right)^{7/16} \Rightarrow \frac{|d_k(p)|^{7/32}}{U^{1/2}} \ll \frac{p^{7/16}}{k^{7/16}U^{1/2}}.$$

2.

$$\begin{aligned}\sum_{\substack{k\leq 2x\\(k,2r)=1}}\frac{1}{k}\sum_{\substack{B(r)<p\leq\sqrt{x}\\p\equiv A \pmod B\\4p^2\equiv r^2 \pmod{k^2}}}\frac{p^{7/16}\log p}{k^{7/16}U^{1/2}} &\ll \frac{1}{U^{1/2}}\sum_{p\leq\sqrt{x}} p^{7/16}\log p\\ &\ll \frac{1}{U^{1/2}}\sqrt{x^{7/16}}\log x\frac{\sqrt{x}}{\log x}\\ &\ll \frac{x^{23/32}}{U^{1/2}}.\end{aligned}$$

Therefore, substituting the identity (3.13) and choosing

$$U > x^{7/16}\log^{2c} x$$

we obtain

$$\sum_{\substack{k\le 2x\\(k,2r)=1}}\frac{1}{k}\sum_{\substack{B(r)<p\le\sqrt{x}\\p\equiv A \pmod B\\4p^2\equiv r^2 \pmod{k^2}}} L(1,\chi_{d_k(p)})\log p$$

$$=\sum_{\substack{k\le 2x\\(k,2r)=1}}\frac{1}{k}\sum_{\substack{B(r)<p\le\sqrt{x}\\p\equiv A \pmod B\\4p^2\equiv r^2 \pmod{k^2}}}\left[\sum_{n\in\mathbb{N}}\left(\frac{d_k(p)}{n}\right)\frac{e^{-n/U}}{n}+\mathrm{O}\left(\frac{p^{7/16}}{k^{7/16}U^{1/2}}\right)\right]\log p$$

$$=\sum_{\substack{k\le 2x\\(k,2r)=1}}\frac{1}{k}\sum_{\substack{B(r)<p\le\sqrt{x}\\p\equiv A \pmod B\\4p^2\equiv r^2 \pmod{k^2}}}\sum_{n\in\mathbb{N}}\left(\frac{d_k(p)}{n}\right)\frac{e^{-n/U}}{n}\log p+\mathrm{O}\left(\frac{\sqrt{x}}{\log^c x}\right)$$

Throughout the next several pages we continue to make estimates involved with the double sum above. Since we have incurred an error of $\sqrt{x}/\log^c x$ we will choose any free parameters wisely so that our main term is bigger than $\sqrt{x}/\log^c x$. Next we show that we may neglect the larger values of k. Let V be a parameter to be determined. Note that

$$\sum_{\substack{V\le k\le 2x\\(k,2r)=1}}\frac{1}{k}\sum_{n\in\mathbb{N}}\frac{e^{-n/U}}{n}\sum_{\substack{B(r)<p\le\sqrt{x}\\p\equiv A \pmod B\\4p^2\equiv r^2 \pmod{k^2}}}\left(\frac{d_k(p)}{n}\right)\log p$$

$$\ll\log x\sum_{n\in\mathbb{N}}\frac{e^{-n/U}}{n}\sum_{\substack{V\le k\le 2x\\(k,2r)=1}}\frac{1}{k}\sum_{\substack{m\le\sqrt{x}\\4m^2\equiv r^2 \pmod{k^2}}}1$$

$$\ll\log x\sum_{n\in\mathbb{N}}\frac{e^{-n/U}}{n}\sum_{\substack{V\le k\le 2x\\(k,2r)=1}}\frac{\#\{h\in\mathbb{Z}/k^2\mathbb{Z}:4h^2\equiv r^2 \pmod{k^2}\}}{k}\frac{\sqrt{x}}{k^2}$$

In order to find $\#\{h\in\mathbb{Z}/k^2\mathbb{Z}:4h^2\equiv r^2 \pmod{k^2}\}$, suppose $k=p_1^{a_1}p_2^{a_2}\cdots p_t^{a_t}$ where the p_i's are distinct odd primes. Notice that $r^2\equiv(2x_i)^2 \pmod{p_i^{2a_i}}$ has two nonzero solutions whenever $(k,r)=1$. Now use the Chinese Remainder Theorem to solve

$$X=\begin{cases}x_1 & (\mathrm{mod}\ p_1^{a_1})\\ \vdots & \\ x_t & (\mathrm{mod}\ p_t^{a_t}).\end{cases}$$

Thus, $4X^2 \equiv r^2 \pmod{k^2}$ has at most $2^{\nu(k)}$ solutions X modulo k^2 when k is odd, where $\nu(k)$ is the number of distinct prime divisors of k. Therefore,

$$\begin{aligned}
&\log x \sum_{n\in\mathbb{N}} \frac{e^{-n/U}}{n} \sum_{\substack{V\le k\le 2x\\(k,2r)=1}} \frac{\#\{h \in \mathbb{Z}/k^2\mathbb{Z} : 4h^2 \equiv r^2 \pmod{k^2}\}}{k} \frac{\sqrt{x}}{k^2} \\
&\ll \sqrt{x}\log x \sum_{n\in\mathbb{N}} \frac{e^{-n/U}}{n} \sum_{V\le k\le 2x} \frac{2^{\nu(k)}}{k^3} \qquad (3.14)
\end{aligned}$$

To estimate $\sum_{V\le k\le 2x} \frac{2^{\nu(k)}}{k^3}$ we use [34, Exercise 2, pg 53], which states

$$\sum_{m\le T} 2^{\nu(m)} = \frac{6}{\pi^2} T\log T + \mathrm{O}(T)$$

along with the partial summation formula (see pg. 79). Setting $a_n = 2^{\nu(n)}$, $f(y) = \frac{1}{y^3}$ partial summation gives

$$\begin{aligned}
\sum_{k=V}^{2x} \frac{2^{\nu(k)}}{k^3} &= \left(\frac{6}{\pi^2} 2x\log(2x) + \mathrm{O}(2x)\right) \frac{1}{(2x)^3} + \int_V^{2x} \left(\frac{6}{\pi^2} y\log y + \mathrm{O}(y)\right) \frac{3}{y^2}\ \mathrm{dy} \\
&\quad - \left(\frac{6}{\pi^2}(V-1)\log(V-1) + \mathrm{O}(V-1)\right) \frac{1}{V^3} \ll \frac{\log V}{V^2}. \qquad (3.15)
\end{aligned}$$

To estimate the sum $\sum_{n\in\mathbb{N}} \frac{e^{-n/U}}{n}$ we first use the Maclaurin series for e^z and the Alternating Series Estimation Theorem to see that

$$\begin{aligned}
1 - e^{-1/U} &= 1 - \sum_{i=0}^{\infty} \frac{(-1)^i}{U^i i!} \\
&= \frac{1}{U} - \sum_{i=2}^{\infty} \frac{(-1)^i}{U^i i!} \\
&= \frac{1}{U} - \frac{1}{2U^2} + \frac{1}{6U^3} - \frac{1}{24U^4} + \cdots \\
&> \frac{1}{U} - \frac{1}{2U^2}.
\end{aligned}$$

Then using the Maclaurin Series for $-\log(1-z)$ we write

$$\begin{aligned}
\sum_{n\in\mathbb{N}} \frac{e^{-n/U}}{n} &= -\log(1-e^{-1/U}) \\
&\leq -\log\left(\frac{1}{U}-\frac{1}{2U^2}\right) \\
&= -\log\left(\frac{1}{U}\left(1-\frac{1}{2U}\right)\right) \\
&= \log U - \log\left(\frac{2U-1}{2U}\right) \\
&= \log U + \log\left(\frac{2U}{2U-1}\right) \\
&\leq \log U + \log(2) \qquad \text{for } U > 1
\end{aligned} \tag{3.16}$$

Choose

$$V > (\log x)^{(c+3)/2}$$

and use (3.15) and (3.16), to see that (3.14) becomes

$$\begin{aligned}
\sqrt{x}\log x \sum_{n\in\mathbb{N}} \frac{e^{-n/U}}{n} \sum_{V\leq k\leq 2x} \frac{2^{\nu(k)}}{k^3} &\ll \sqrt{x}\log x(\log U)\left(\frac{\log V}{V^2}\right) \\
&\ll \sqrt{x}\log x(\log U)\left(\frac{1}{V^{2-\epsilon_1}}\right) \\
&\ll \sqrt{x}\log x(\log U)\left(\frac{1}{(\log x)^{c+3-\epsilon_2}}\right) \\
&\ll \frac{\sqrt{x}}{(\log x)^{c+2-\epsilon_2}}(\log U) \\
&\ll \frac{\sqrt{x}}{(\log x)^{c+1-\epsilon_2}} \\
&\ll \frac{\sqrt{x}}{\log^c x}
\end{aligned}$$

if $U \ll \sqrt{x}/\log x$. Note that requiring this upper bound on U will not be a problem since we will soon choose U to be a function of x which is $\ll \sqrt{x}/\log x$. We have shown

that

$$\begin{aligned}&\sum_{\substack{k\le 2x\\(k,2r)=1}}\frac{1}{k}\sum_{\substack{B(r)<p\le\sqrt{x}\\p\equiv A\pmod B\\4p^2\equiv r^2\pmod{k^2}}}L(1,\chi_{d_k(p)})\log p\\&=\sum_{\substack{k\le V\\(k,2r)=1}}\frac{1}{k}\sum_{n\in\mathbb{N}}\frac{e^{-n/U}}{n}\sum_{\substack{B(r)<p\le\sqrt{x}\\p\equiv A\pmod B\\4p^2\equiv r^2\pmod{k^2}}}\left(\frac{d_k(p)}{n}\right)\log p+\mathrm{O}\left(\frac{\sqrt{x}}{\log^c x}\right)\end{aligned}\tag{3.17}$$

Now we concentrate of large values of n. Note that

$$\sum_{n\ge U\log U}\frac{e^{-n/U}}{n}\ll\sum_{n\ge U\log U}\frac{e^{-n/U}}{U\log U}\ll\frac{1}{U\log U}\int_{U\log U}^{\infty}e^{-x/U}dx=\frac{1}{U\log U}$$

and recall that U has been chosen so that

$$U>x^{7/16}\log^{2c}x.$$

Therefore,

$$\begin{aligned}&\sum_{\substack{k\le V\\(k,2r)=1}}\frac{1}{k}\sum_{n\ge U\log U}\frac{e^{-n/U}}{n}\sum_{\substack{B(r)<p\le\sqrt{x}\\p\equiv A\pmod B\\4p^2\equiv r^2\pmod{k^2}}}\left(\frac{d_k(p)}{n}\right)\log p\\&\ll\frac{\log x}{U\log U}\sum_{\substack{k\le V\\(k,2r)=1}}\frac{1}{k}\sum_{\substack{m\le\sqrt{x}\\4m^2\equiv r^2\pmod{k^2}}}1\\&\ll\frac{\sqrt{x}\log x}{U\log U}\ll\frac{\sqrt{x}}{\log^c x}.\end{aligned}$$

Substituting this into (3.17) we obtain

$$\begin{aligned}&\sum_{\substack{k\le 2x\\(k,2r)=1}}\frac{1}{k}\sum_{\substack{B(r)<p\le\sqrt{x}\\p\equiv A\pmod B\\4p^2\equiv r^2\pmod{k^2}}}L(1,\chi_{d_k(p)})\log p\\&=\sum_{\substack{k\le V\\(k,2r)=1}}\frac{1}{k}\sum_{n<U\log U}\frac{e^{-n/U}}{n}\sum_{\substack{B(r)<p\le\sqrt{x}\\p\equiv A\pmod B\\4p^2\equiv r^2\pmod{k^2}}}\left(\frac{d_k(p)}{n}\right)\log p+\mathrm{O}\left(\frac{\sqrt{x}}{\log^c x}\right).\end{aligned}\tag{3.18}$$

For the inner sum

$$\sum_{\substack{B(r)<p\le\sqrt{x}\\ p\equiv A \pmod B\\ 4p^2\equiv r^2 \pmod{k^2}}} \left(\frac{d_k(p)}{n}\right)\log p$$

note that $\left(\frac{d_k(p)}{\bullet}\right)$ is periodic modulo $4n$. That is,

$$d_1 \equiv d_2 \pmod{4n} \Rightarrow \left(\frac{d_1}{n}\right) = \left(\frac{d_2}{n}\right) \qquad \text{for all } n \in \mathbb{N}$$

Thus

$$\begin{aligned}&\sum_{\substack{B(r)<p\le\sqrt{x}\\ p\equiv A \pmod B\\ 4p^2\equiv r^2 \pmod{k^2}}} \left(\frac{d_k(p)}{n}\right)\log p\\ &= \sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*}\left(\frac{a}{n}\right) \sum_{\substack{B(r)<p\le\sqrt{x}\\ p\equiv A \pmod B\\ 4p^2\equiv r^2 \pmod{k^2}\\ d_k(p)=(r^2-4p^2)/k^2\equiv a \pmod{4n}}} \log p.\end{aligned}$$

For positive coprime integers C and D define

$$\psi_1(X,C,D) := \sum_{\substack{2\le p\le X\\ p\equiv D \pmod C}} \log p.$$

Then

$$\begin{aligned}&\sum_{\substack{B(r)<p\le\sqrt{x}\\ p\equiv A \pmod B\\ 4p^2\equiv r^2 \pmod{k^2}}} \left(\frac{d_k(p)}{n}\right)\log p\\ &= \sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*}\left(\frac{a}{n}\right) \sum_{\substack{b\in\left(\mathbb{Z}/4Bnk^2\mathbb{Z}\right)^*\\ b\equiv A \pmod B\\ 4b^2\equiv r^2-ak^2 \pmod{4nk^2}}} \psi_1(\sqrt{x},4Bnk^2,b) + \mathrm{O}\left(\frac{2^{\nu(nk)}}{Bk^2}\right)\end{aligned}$$

where the O-term comes from the following estimates.

$$\begin{aligned}
&\sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*}\left(\frac{a}{n}\right)\sum_{\substack{b\in\left(\mathbb{Z}/4Bnk^2\mathbb{Z}\right)^*\\ b\equiv A \pmod B\\ 4b^2\equiv r^2-ak^2 \pmod{4nk^2}}}\sum_{\substack{2\le p\le B(r)\\ p\equiv b \pmod{4Bnk^2}}}\log p\\
&\ll \sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*}\left(\frac{a}{n}\right)\sum_{\substack{b\in\left(\mathbb{Z}/4Bnk^2\mathbb{Z}\right)^*\\ b\equiv A \pmod B\\ 4b^2\equiv r^2-ak^2 \pmod{4nk^2}}}\frac{B(r)}{4Bnk^2}\log(B(r))\\
&\ll \sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*}\left(\frac{a}{n}\right)\frac{2^{\nu(nk)}}{4Bnk^2}\\
&\ll \frac{2^{\nu(nk)}}{Bk^2}\cdot\frac{\phi(4n)}{4n}\\
&\ll \frac{2^{\nu(nk)}}{Bk^2}.
\end{aligned}$$

Since $\psi_1(X,C,D)\sim\frac{X}{\phi(C)}$ (see [34, Chapter 2 §8.2 Theorem 5]) we define

$$E_1(X,C,D):=\psi_1(X,C,D)-\frac{X}{\phi(C)}.$$

Therefore,

$$\begin{aligned}
&\sum_{\substack{B(r)<p\le\sqrt{x}\\ p\equiv A \pmod B\\ 4p^2\equiv r^2 \pmod{k^2}}}\left(\frac{d_k(p)}{n}\right)\log p\\
&=\sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*}\left(\frac{a}{n}\right)\sum_{\substack{b\in\left(\mathbb{Z}/4Bnk^2\mathbb{Z}\right)^*\\ b\equiv A \pmod B\\ 4b^2\equiv r^2-ak^2 \pmod{4nk^2}}}\left[\frac{\sqrt{x}}{\phi(4Bnk^2)}+E_1(\sqrt{x},4Bnk^2,b)\right]\\
&\quad+\mathrm{O}\left(\frac{2^{\nu(nk)}}{Bk^2}\right)\\
&=\sqrt{x}\sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*}\left(\frac{a}{n}\right)\frac{C_r(a,n,k)}{\phi(4Bnk^2)}\\
&\quad+\sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*}\left(\frac{a}{n}\right)\sum_{\substack{b\in\left(\mathbb{Z}/4Bnk^2\mathbb{Z}\right)^*\\ b\equiv A \pmod B\\ 4b^2\equiv r^2-ak^2 \pmod{4nk^2}}}E_1(\sqrt{x},4Bnk^2,b)+\mathrm{O}\left(\frac{2^{\nu(nk)}}{Bk^2}\right)
\end{aligned}$$

where as before

$$C_r(a,n,k) =$$
$$\#\{b \in (\mathbb{Z}/4Bnk^2\mathbb{Z})^* : b \equiv A \pmod{B}; 4b^2 \equiv r^2 - ak^2 \pmod{4nk^2}\}.$$

If we interchange the sum on $a \in (\mathbb{Z}/4n\mathbb{Z})^*$ with the sum on $b \in (\mathbb{Z}/4Bnk^2\mathbb{Z})^*$, then for a fixed b there is at most one value of $a \in (\mathbb{Z}/4n\mathbb{Z})^*$ such that $4b^2 \equiv r^2 - ak^2 \pmod{4nk^2}$. Therefore,

$$\begin{aligned}
&\left| \sum_{a \in (\mathbb{Z}/4n\mathbb{Z})^*} \left(\frac{a}{n}\right) \sum_{\substack{b \in \left(\mathbb{Z}/4Bnk^2\mathbb{Z}\right)^* \\ b \equiv A \pmod{B} \\ 4b^2 \equiv r^2 - ak^2 \pmod{4nk^2}}} E_1(\sqrt{x}, 4Bnk^2, b) \right| \\
&\leq \left| \sum_{\substack{b \in \left(\mathbb{Z}/4Bnk^2\mathbb{Z}\right)^* \\ b \equiv A \pmod{B}}} E_1(\sqrt{x}, 4Bnk^2, b) \sum_{\substack{a \in (\mathbb{Z}/4n\mathbb{Z})^* \\ 4b^2 \equiv r^2 - ak^2 \pmod{4nk^2}}} \left(\frac{a}{n}\right) \right| \\
&\leq \sum_{\substack{b \in \left(\mathbb{Z}/4Bnk^2\mathbb{Z}\right)^* \\ b \equiv A \pmod{B}}} \left| E_1(\sqrt{x}, 4Bnk^2, b) \cdot 1 \right| \\
&\leq \sum_{b \in (\mathbb{Z}/4Bnk^2\mathbb{Z})^*} \left| E_1(\sqrt{x}, 4Bnk^2, b) \right|.
\end{aligned}$$

Hence,

$$\begin{aligned}
&\sum_{a \in (\mathbb{Z}/4n\mathbb{Z})^*} \left(\frac{a}{n}\right) \sum_{\substack{b \in \left(\mathbb{Z}/4Bnk^2\mathbb{Z}\right)^* \\ b \equiv A \pmod{B} \\ 4b^2 \equiv r^2 - ak^2 \pmod{4nk^2}}} E_1(\sqrt{x}, 4Bnk^2, b) \\
&\ll \sum_{b \in (\mathbb{Z}/4Bnk^2\mathbb{Z})^*} \left| E_1(\sqrt{x}, 4Bnk^2, b) \right|.
\end{aligned}$$

Therefore, we may write (3.18) on page 94 as

$$\begin{aligned}
&\sum_{\substack{k\le 2x\\(k,2r)=1}} \frac{1}{k} \sum_{\substack{B(r)<p\le\sqrt{x}\\ p\equiv A \pmod B\\ 4p^2\equiv r^2 \pmod{k^2}}} L(1,\chi_{d_k(p)})\log p \\
&= \sum_{\substack{k\le V\\(k,2r)=1}} \frac{1}{k} \sum_{n<U\log U} \frac{e^{-n/U}}{n}\Bigg[\sqrt{x}\sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*}\left(\frac{a}{n}\right)\frac{C_r(a,n,k)}{\phi(4Bnk^2)} \\
&\qquad + \sum_{b\in(\mathbb{Z}/4Bnk^2\mathbb{Z})^*} \left|E_1(\sqrt{x},4Bnk^2,b)\right| + \mathrm{O}\left(\frac{2^{\nu(nk)}}{Bk^2}\right)\Bigg] + \mathrm{O}\left(\frac{\sqrt{x}}{\log^c x}\right)
\end{aligned} \tag{3.19}$$

For the O-term inside the brackets note that for any $\epsilon > 0$

$$2^{\nu(m)} = \sum_{\substack{d\mid m\\ d \text{ squarefree}}} 1 \le \sum_{d\mid m} 1 \ll (m)^{\epsilon}$$

(see pg. 81). With this fact we have for any $\epsilon > 0$

$$\begin{aligned}
\sum_{\substack{k\le V\\(k,2r)=1}} \sum_{n<U\log U} \frac{e^{-n/U}2^{\nu(nk)}}{nk^3} &\ll \sum_{k\le V}\frac{k^{\epsilon}}{k^3}\sum_{n<U\log U}\frac{e^{-n/U}n^{\epsilon}}{n} \\
&\ll \sum_{k\le V}\frac{1}{k^{3-\epsilon}}\sum_{n<U\log U}\mathrm{O}(1) \\
&\ll U\log U
\end{aligned}$$

and

$$U\log U \ll \frac{\sqrt{x}}{\log^c x}$$

when

$$U \ll \frac{\sqrt{x}}{\log^{c+1} x}.$$

Therefore, (3.19) becomes

$$\begin{aligned}
&\sum_{\substack{k\le 2x\\(k,2r)=1}}\frac{1}{k}\sum_{\substack{B(r)<p\le\sqrt{x}\\p\equiv A \pmod B\\4p^2\equiv r^2 \pmod{k^2}}} L(1,\chi_{d_k(p)})\log p\\
&=\sum_{\substack{k\le V\\(k,2r)=1}}\frac{1}{k}\sum_{n<U\log U}\frac{e^{-n/U}}{n}\Bigg[\sqrt{x}\sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*}\left(\frac{a}{n}\right)\frac{C_r(a,n,k)}{\phi(4Bnk^2)} \qquad (3.20)\\
&\quad+\sum_{b\in(\mathbb{Z}/4Bnk^2\mathbb{Z})^*}\left|E_1(\sqrt{x},4Bnk^2,b)\right|\Bigg]+\mathrm{O}\left(\frac{\sqrt{x}}{\log^c x}\right).
\end{aligned}$$

Recall the Cauchy-Schwarz inequality. For two real valued sequences $\{a_n\}$ and $\{b_n\}$,

$$\sum_n a_n b_n \le \left(\sum_n a_n^2\right)^{1/2}\left(\sum_n b_n^2\right)^{1/2}.$$

We apply the Cauchy-Schwarz inequality to the middle term of (3.20) and obtain

$$\begin{aligned}
&\sum_{\substack{k\le V\\(k,2r)=1}}\frac{1}{k}\sum_{\substack{n\le U\log U\\b\in(\mathbb{Z}/4Bnk^2\mathbb{Z})^*}}\frac{e^{-n/U}}{n}|E_1(\sqrt{x},4Bnk^2,b)| \qquad (3.21)\\
&\le\sum_{k\le V}\frac{1}{k}\left(\sum_{n\le U\log U}\frac{\phi(4Bnk^2)}{n^2}\right)^{1/2}\left(\sum_{n\le U\log U}\sum_{b\in(\mathbb{Z}/4Bnk^2\mathbb{Z})^*}E_1(\sqrt{x},4Bnk^2,b)^2\right)^{1/2}
\end{aligned}$$

Using the identity $\phi(AB) = \phi(A)\phi(B)\frac{(A,B)}{\phi((A,B))}$ we can write,

$$\begin{aligned}
&\sum_{k\le V}\frac{1}{k}\left(\sum_{n\le U\log U}\frac{\phi(4Bnk^2)}{n^2}\right)^{1/2}\left(\sum_{n\le U\log U}\sum_{b\in(\mathbb{Z}/4Bnk^2\mathbb{Z})^*}E_1(\sqrt{x},4Bnk^2,b)^2\right)^{1/2}\\
&=\sum_{k\le V}\frac{\sqrt{\phi(k^2)}}{k}\left(\sum_{n\le U\log U}\frac{\phi(4Bn)}{n^2}\frac{(4Bn,k^2)}{\phi((4Bn,k^2))}\right)^{1/2}\\
&\qquad\cdot\left(\sum_{n\le U\log U}\sum_{b\in(\mathbb{Z}/4Bnk^2\mathbb{Z})^*}E_1(\sqrt{x},4Bnk^2,b)^2\right)^{1/2}\\
&=\phi(B)\sum_{k\le V}\frac{\sqrt{\phi(k^2)}}{k}\left(\sum_{n\le U\log U}\frac{\phi(4n)}{n^2}\frac{(4n,B)}{\phi((4n,B))}\frac{(4Bn,k^2)}{\phi((4Bn,k^2))}\right)^{1/2}\\
&\qquad\cdot\left(\sum_{n\le U\log U}\sum_{b\in(\mathbb{Z}/4Bnk^2\mathbb{Z})^*}E_1(\sqrt{x},4Bnk^2,b)^2\right)^{1/2}
\end{aligned}$$

Note that $\phi(4n)\le 4\phi(n)$, $\phi(k^2)=k\phi(k)$, $\phi(n)\le n$, and

$$\frac{(4Bn,k^2)}{\phi((4Bn,k^2))}=\prod_{p|(4Bn,k^2)}\frac{p}{p-1}\le\prod_{p|(4Bn,k^2)}2=2^{\nu((4Bn,k^2))}\le 2^{\nu(k)}.$$

Similiarly,

$$\frac{(4n,B)}{\phi((4n,B))}\le 2^{\nu(B)}.$$

Recall that for any $\epsilon>0$, $2^{\nu(m)}\le m^{\epsilon}$ (see pg. 81). Therefore,

$$\begin{aligned}
&\sum_{k\le V}\frac{1}{k}\left(\sum_{n\le U\log U}\frac{\phi(4Bnk^2)}{n^2}\right)^{1/2}\left(\sum_{n\le U\log U}\sum_{b\in(\mathbb{Z}/4Bnk^2\mathbb{Z})^*}E_1(\sqrt{x},4Bnk^2,b)^2\right)^{1/2}\\
&\ll\sum_{k\le V}\sqrt{2^{\nu(k)}2^{\nu(B)}}\left(\sum_{n\le U\log U}\frac{1}{n}\right)^{1/2}\left(\sum_{n\le U\log U}\sum_{b\in(\mathbb{Z}/4Bnk^2\mathbb{Z})^*}E_1(\sqrt{x},4Bnk^2,b)^2\right)^{1/2}\\
&\ll\sum_{k\le V}\sqrt{k^{\epsilon}}(\log U)^{1/2}\left(\sum_{n\le U\log U}\sum_{b\in(\mathbb{Z}/4Bnk^2\mathbb{Z})^*}E_1(\sqrt{x},4Bnk^2,b)^2\right)^{1/2}
\end{aligned}$$

Substituting $m = 4Bnk^2$ (3.21) may be written as

$$\sum_{\substack{k\leq V\\(k,2r)=1}} \frac{1}{k} \sum_{\substack{n\leq U\log U\\ b\in(\mathbb{Z}/4Bnk^2\mathbb{Z})^*}} \frac{e^{-n/U}}{n}|E_1(\sqrt{x},4Bnk^2,b)|$$
$$\ll \sqrt{\log U}\sum_{k\leq V}\sqrt{k^\epsilon}\left(\sum_{m\leq 4BV^2U\log U}\sum_{b\in(\mathbb{Z}/m\mathbb{Z})^*} E_1(\sqrt{x},m,b)^2\right)^{1/2}$$

The Barban, Davenport, Halberstam Theorem asserts that given any $l > 0$ we have for $X > Q > X/\log^l X$

$$\sum_{m\leq Q}\sum_{b\in(\mathbb{Z}/m\mathbb{Z})^*} E_1(X,m,b)^2 \ll QX\log X.$$

Therefore, if $\sqrt{x} > 4BV^2U\log U > \sqrt{x}/\log^l(\sqrt{x})$, then

$$\sqrt{\log U}\sum_{k\leq V}\sqrt{kB}\left(\sum_{m\leq 4BV^2U\log U}\sum_{b\in(\mathbb{Z}/m\mathbb{Z})^*} E_1(\sqrt{x},m,b)^2\right)^{1/2}$$
$$\ll \sqrt{\log U}\sum_{k\leq V}\sqrt{kB}\left(4BV^2U\log U\sqrt{x}\log x\right)^{1/2}$$
$$\ll (\log U)V^3\sqrt{U}\sqrt{\sqrt{x}\log x}$$
$$\ll \frac{\sqrt{x}}{\log^c x}$$

when

$$\begin{aligned} U &= \frac{\sqrt{x}}{\log^{5c+15} x},\\ V &= \log^{(c+3)/2} x. \end{aligned} \tag{3.22}$$

We have shown that (3.19) on page 98 becomes

$$\begin{aligned}&\sum_{\substack{k\le 2x\\(k,2r)=1}}\frac{1}{k}\sum_{\substack{B(r)<p\le\sqrt{x}\\p\equiv A \pmod B\\4p^2\equiv r^2 \pmod{k^2}}} L(1,\chi_{d_k(p)})\log p\\&=\sqrt{x}\sum_{\substack{k\le V\\(k,2r)=1}}\frac{1}{k}\sum_{n\le U\log U}\frac{e^{-n/U}}{n}\sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*}\left(\frac{a}{n}\right)\frac{C_r(a,n,k)}{\phi(4Bnk^2)}+\mathrm{O}\left(\frac{\sqrt{x}}{\log^c x}\right).\end{aligned}\tag{3.23}$$

We now prove

Claim 3.5.1.

$$\begin{aligned}&\sum_{\substack{k\le V\\n\le U\log U\\(k,2r)=1}}\frac{e^{-n/U}}{kn\phi(4Bnk^2)}\sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*}\left(\frac{a}{n}\right)C_r(a,n,k)\\&=\sum_{\substack{k,n\in\mathbb{N}\\(k,2r)=1}}\frac{1}{kn\phi(4Bnk^2)}\sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*}\left(\frac{a}{n}\right)C_r(a,n,k)+\mathrm{O}\left(\frac{1}{\log^c x}\right).\end{aligned}$$

Recall that

$$C_r(a,n,k)=\prod_{p|4Bnk^2}d_p(n)$$

where the $d_p(n)$ are given in Lemma 3.4.2. In particluar, $d_2(n)$ is at most $2^{\mathrm{ord}_2(B)+3}$ by Lemma 3.4.2 (4)-(6). For $p|B$, $d_p(n)$ is at most $p^{\mathrm{ord}_p(B)}$ by Lemma 3.4.2 (1) and (3). For $p|nk$ and $p\nmid B$, $d_p(n)$ is at most 2. Therefore,

$$\begin{aligned}C_r(a,n,k)&=d_2(n)\left(\prod_{\substack{p|B\\p\neq 2}}d_p(n)\right)\left(\prod_{\substack{p|k\\p\nmid 2B}}d_p(n)\right)\left(\prod_{\substack{p|n\\p\nmid 2Bk}}d_p(n)\right)\\&\le 16B2^{\nu(k)}2^{\nu(n)-\nu((n,k))}\\&=16B2^{\nu(nk)}\end{aligned}$$

Since $C_r(a,n,k)=0$ if $a\equiv 3 \pmod 4$,

$$\sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*}\left(\frac{a}{n}\right)C_r(a,n,k)=\sum_{\substack{a\in(\mathbb{Z}/4n\mathbb{Z})^*\\ a\equiv 1 \pmod 4}}\left(\frac{a}{n}\right)C_r(a,n,k)$$
$$\ll \phi(n)2^{\nu(nk)}. \tag{3.24}$$

Therefore,

$$\sum_{\substack{k\le V\\ n\le U\log U\\ (k,2r)=1}}\frac{e^{-n/U}}{kn\phi(4Bnk^2)}\sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*}\left(\frac{a}{n}\right)C_r(a,n,k)$$
$$=\sum_{\substack{k\in\mathbb{N}\\ n\le U\log U\\ (k,2r)=1}}\frac{e^{-n/U}}{kn\phi(4Bnk^2)}\sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*}\left(\frac{a}{n}\right)C_r(a,n,k)$$
$$+\mathrm{O}\left(\sum_{\substack{k>V\\ n\le U\log U\\ (k,2r)=1}}\frac{e^{-n/U}\phi(n)2^{\nu(nk)}}{kn\phi(4Bnk^2)}\right).$$

Since $\phi(4Bnk^2)\ge 2\phi(B)\phi(n)\phi(k^2)$ and $2^{\nu(nk)}\le 2^{\nu(n)+\nu(k)}$,

$$\sum_{\substack{k>V\\ (k,2r)=1}}\frac{1}{k}\sum_{n\le U\log U}\frac{e^{-n/U}\phi(n)2^{\nu(nk)}}{n\phi(4Bnk^2)}\le\sum_{k>V}\frac{2^{\nu(k)}}{k\phi(k^2)}\sum_{n\le U\log U}\frac{e^{-n/U}2^{\nu(n)}}{n\phi(B)}$$
$$\ll\sum_{k>V}\frac{2^{\nu(k)}}{k^2\phi(k)}\sum_{n\le U\log U}\frac{e^{-n/U}2^{\nu(n)}}{n} \tag{3.25}$$

We use partial summation (see pg. 79) to estimate the sums in (3.25). To that end, observe that

$$\phi(k)=\prod_{p^\alpha||k}p^{\alpha-1}(p-1)=k\prod_{p|k}\left(1-\frac{1}{p}\right)$$

and if $p>3$, then

$$\frac{2p}{p-1}<3.$$

Therefore,

$$\frac{2^{\nu(k)}}{\phi(k)} = \frac{1}{k}\prod_{p|k}\frac{2}{1-p^{-1}} = \frac{1}{k}\prod_{p|k}\frac{2p}{p-1}$$
$$\leq \frac{4}{k}\prod_{\substack{p|k\\p>2}}\frac{2p}{p-1} \leq \frac{12}{k}\prod_{\substack{p|k\\p>3}}\frac{2p}{p-1} \leq \frac{12}{k}\prod_{\substack{p|k\\p>3}}3 \ll \frac{3^{\nu(k)}}{k}.$$

Thus,

$$\sum_{k>V}\frac{2^{\nu(k)}}{k^2\phi(k)} \ll \sum_{k>V}\frac{3^{\nu(k)}}{k^3}. \tag{3.26}$$

Using [34, Excercise 4, pg 53]

$$\sum_{n\leq T}3^{\nu(n)} \ll T\log^2 T.$$

Set

$$a_n = 3^{\nu(n)};\ f(y) = \frac{1}{y^3}.$$

Then for $X > V+1$ partial summation (see pg. 79) gives

$$\sum_{k=V+1}^{X}\frac{3^{\nu(k)}}{k^3} \ll \frac{\log^2 V}{V^2}$$

Thus,

$$\sum_{k>V}\frac{2^{\nu(k)}}{k^2\phi(k)} \ll \frac{\log^2 V}{V^2}.$$

To estimate $\sum_{n\leq U\log U}\frac{e^{-n/U}2^{\nu(n)}}{n}$ we set

$$a_n = 2^{\nu(n)}; \qquad f(y) = \frac{e^{-y/U}}{y}$$

then using $\sum_{n\leq T} 2^{\nu(n)} \ll T\log T$ from [34, Exercise 2, pg 53], partial summation (see pg. 79) gives

$$\begin{aligned}
&\sum_{n\leq U\log U} \frac{e^{-n/U}2^{\nu(n)}}{n} \\
&\ll \frac{e^{-U(\log U)/U}}{U\log U}\sum_{n\leq U\log U} 2^{\nu(n)} + \int_1^{U\log U} (t\log t)\left[\frac{e^{-t/U}}{t^2}+\frac{e^{-t/U}}{tU}\right]\,\mathrm{dt} \\
&\ll \frac{\log U}{U} + \int_1^{U\log U} \frac{e^{-t/U}\log t}{t}\,\mathrm{dt} + \int_1^{U\log U}\frac{e^{-t/U}\log t}{U}\,\mathrm{dt} \\
&\ll \frac{\log U}{U} + \int_1^{U\log U}\frac{\log t}{t}\,\mathrm{dt} + \frac{1}{U}\int_1^{U\log U}\log t\,\mathrm{dt} \\
&\ll \frac{\log U}{U} + \log^2 U + \frac{1}{U}\log U\int_1^{U\log U} 1\,\mathrm{dt} \\
&\ll \log^2 U.
\end{aligned} \tag{3.27}$$

Replacing the two sums in (3.25) with the estimates given in (3.26) and (3.27) gives

$$\begin{aligned}
\sum_{\substack{k>V\\ n\leq U\log U\\ (k,2r)=1}} \frac{e^{-n/U}\phi(n)2^{\nu(nk)}}{n\phi(4Bnk^2)} &\ll \left(\frac{\log^2 V}{V^2}\right)\log^2 U \\
&\ll \frac{(\log\log x)^2}{\log^{c+3} x}\log^2 x \\
&\ll \frac{1}{\log^c x}
\end{aligned}$$

as U and V are given by (3.22). We have shown that

$$\begin{aligned}
&\sum_{\substack{k\leq V\\ n\leq U\log U\\ (k,2r)=1}} \frac{e^{-n/U}}{kn\phi(4Bnk^2)}\sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*}\left(\frac{a}{n}\right)C_r(a,n,k) \\
&= \sum_{\substack{k\in\mathbb{N}\\ n\leq U\log U\\ (k,2r)=1}} \frac{e^{-n/U}}{kn\phi(4Bnk^2)}\sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*}\left(\frac{a}{n}\right)C_r(a,n,k) \\
&\quad + \mathrm{O}\left(\frac{1}{\log^c x}\right)
\end{aligned}$$

whenever U and V are given by (3.22). Furthermore,

$$\sum_{\substack{k\in\mathbb{N}\\ n\leq U\log U\\ (k,2r)=1}} \frac{e^{-n/U}}{kn\phi(4Bnk^2)} \sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*} \left(\frac{a}{n}\right) C_r(a,n,k)$$

$$= \sum_{\substack{k\in\mathbb{N}\\ (k,2r)=1}} \sum_{n=1}^{\infty} \frac{e^{-n/U}}{kn\phi(4Bnk^2)} \sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*} \left(\frac{a}{n}\right) C_r(a,n,k) +$$

$$\mathrm{O}\left(\sum_{k\in\mathbb{N}} \frac{2^{\nu(k)}}{k\phi(k^2)} \sum_{n>U\log U} \frac{e^{-n/U}2^{\nu(n)}}{n}\right)$$

Recall that for any $\epsilon > 0$

$$2^{\nu(m)} \ll (m)^{\epsilon}$$

(see pg. 98). Thus the error term above is

$$\ll \frac{1}{\sqrt{U\log U}} \int_{U\log U}^{\infty} e^{-t/U}\ \mathrm{dt} \ll \frac{1}{\log^c x}.$$

Recall the statement of Claim 3.5.1

$$\sum_{\substack{k\leq V\\ n\leq U\log U\\ (k,2r)=1}} \frac{e^{-n/U}}{kn\phi(4Bnk^2)} \sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*} \left(\frac{a}{n}\right) C_r(a,n,k)$$

$$= \sum_{\substack{k,n\in\mathbb{N}\\ (k,2r)=1}} \frac{1}{kn\phi(4Bnk^2)} \sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*} \left(\frac{a}{n}\right) C_r(a,n,k) + \mathrm{O}\left(\frac{1}{\log^c x}\right).$$

Use the identity

$$\sum_{\substack{k\in\mathbb{N}\\ (k,2r)=1}} \sum_{n=1}^{\infty} \frac{e^{-n/U}}{kn\phi(4Bnk^2)} \sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*} \left(\frac{a}{n}\right) C_r(a,n,k)$$

$$= \sum_{\substack{k\in\mathbb{N}\\ (k,2r)=1}} \sum_{n=1}^{\infty} \frac{1}{kn\phi(4Bnk^2)} \sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*} \left(\frac{a}{n}\right) C_r(a,n,k) + \mathrm{O}\left(\frac{1}{\log^c x}\right) \quad (3.28)$$

(see [8, pg. 15]). Claim 3.5.1 follows. Using (3.24) and $\phi(k^2) = k\phi(k)$ we may write

$$\sum_{\substack{k\leq V\\ n\leq U\log U\\ (k,2r)=1}} \frac{e^{-n/U}}{kn\phi(4Bnk^2)} \sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*} \left(\frac{a}{n}\right) C_r(a,n,k) \leq \sum_{\substack{k\leq V\\ n\leq U\log U\\ (k,2r)=1}} \frac{e^{-n/U}\phi(n)2^{\nu(nk)}}{k^2n\phi(4Bnk)}$$

We make the following two observations:

1. For any $\epsilon > 0$, $2^{\nu(nk)} \ll (nk)^{\epsilon}$.
2. $\phi(4Bnk) \geq \phi(n)\phi(4Bk)$.

Therefore, for any $\epsilon > 0$

$$\sum_{\substack{k\leq V\\ n\leq U\log U\\ (k,2r)=1}} \frac{e^{-n/U}\phi(n)2^{\nu(nk)}}{k^2n\phi(4Bnk)} \leq \sum_{\substack{k\leq V\\ n\leq U\log U\\ (k,2r)=1}} \frac{e^{-n/U}}{n^{1-\epsilon}k^{2-\epsilon}\phi(4Bk)}.$$

The double sum above is

$$\ll \left(\sum_{n\geq 1} \frac{e^{-n/U}}{n^{1-\epsilon}}\right)\left(\sum_{k\geq 1} \frac{1}{k^{2-\epsilon}\phi(4Bk)}\right) \ll \sum_{n\geq 1} \frac{e^{-n/U}}{n^{1-\epsilon}} \ll \sum_{n\geq 1} e^{-n/U} \ll 1$$

Therefore, using Claim 3.5.1 the double sum

$$\sum_{\substack{k,n\in\mathbb{N}\\ (k,2r)=1}} \frac{1}{kn\phi(4Bnk^2)} \sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*} \left(\frac{a}{n}\right) C_r(a,n,k)$$

converges. Thus, (3.23) from page 102 becomes

$$\sum_{\substack{k\leq 2x\\ (k,2r)=1}} \frac{1}{k} \sum_{\substack{B(r)<p\leq\sqrt{x}\\ p\equiv A \pmod B\\ 4p^2\equiv r^2 \pmod{k^2}}} L(1,\chi_{d_k(p)})\log p$$
$$= \sqrt{x}\left[\sum_{k=1}^{\infty}\frac{1}{k}\sum_{n=1}^{\infty}\frac{1}{n\phi(4Bnk^2)} \sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*}\left(\frac{a}{n}\right)C_r(a,n,k)\right] + \mathrm{O}\left(\frac{\sqrt{x}}{\log^c x}\right).$$

□

Recall that

$$C_{r,A,B} = \sum_{\substack{k\in\mathbb{N}\\(k,2r)=1}} \frac{1}{k}\sum_{n=1}^{\infty} \frac{1}{n\phi(4nBk^2)} \sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*} \left(\frac{a}{n}\right) C_r(a,n,k)$$

where

$$C_r(a,n,k) =$$

$$\#\{b \in (\mathbb{Z}/4Bnk^2\mathbb{Z})^* : b \equiv A \pmod{B}; 4b^2 \equiv r^2 - ak^2 \pmod{4nk^2}\}.$$

In this section we construct a multiplicative function which is a necessary tool used to prove a product formula for $C_{r,A,B}$ which in turn gives the constant in Theorem 3.0.17 (2). Recall that before we computed $C_r(a,n,k)$ in section 3.4 we used the Chinese Remainder Theorem (see pg. 84) to write

$$C_r(a,n,k) = \prod_{\substack{p|(4Bnk^2)\\p \text{ prime}}} d_p(n)$$

where

$$d_p(n) = \sum_{\substack{b\in(\mathbb{Z}/p^{\mathrm{ord}_p(4Bnk^2)}\mathbb{Z})^*\\ b\equiv A \pmod{p^{\mathrm{ord}_p(B)}}\\ 4b^2\equiv r^2-ak^2 \pmod{p^{\mathrm{ord}_p(4nk^2)}}}} 1$$

Let

$$e_2(n) = \begin{cases} \frac{d_2(n)}{d_2(1)} & \text{if } d_2(1)\neq 0 \\ 0 & \text{if } d_2(1) = 0. \end{cases}$$

Definition 3.6.1. *Set* $n = 2^{\mathrm{ord}_2 n} n'$.

$$c_k(n) = \sum_{\substack{a\in(\mathbb{Z}/4n\mathbb{Z})^*\\ a\equiv 1 \pmod 4\\ (r^2-ak^2,n')=1}} \left(\frac{a}{n}\right) e_2(n) \prod_{\substack{p|n\\p\neq 2}} d_p(n)$$

Lemma 3.6.2. *Let q be an odd prime. For $\alpha > 0$,*

1. *$c_k(n)$ is a multiplicative function in n and $c_k(1) = 1$.*
2. *Suppose $q|B$ and write $k = q^\beta k_1$, where $\mathrm{ord}_q(k) = \beta$.*
   (a) *If $2\beta \geq \mathrm{ord}_q(B)$, then*
   $$c_k(q^\alpha) = \begin{cases} q^{\mathrm{ord}_q(B)}\phi(q^\alpha) & \text{if } r^2 \equiv 4A^2 \pmod{q^{\mathrm{ord}_q(B)}} \\ & \text{and } \alpha \text{ is even} \\ 0 & \text{otherwise.} \end{cases}$$
   (b) *If $2\beta < \mathrm{ord}_q(B)$, then*
   $$c_k(q^\alpha) = \begin{cases} q^{\alpha - \min(\alpha, \mathrm{ord}_q(B) - 2\beta)} \left(\frac{(r^2 - 4A^2)/q^{2\beta}}{q}\right)^\alpha & \text{if } r^2 \equiv 4A^2 \pmod{q^{2\beta}} \\ 0 & \text{otherwise.} \end{cases}$$
3. *Suppose $q \nmid B$.*
   (a) *If $q|k$, then*
   $$c_k(q^\alpha) = \begin{cases} 2q^{\alpha-1}(q-1) & \text{if } \alpha \text{ is even} \\ 0 & \text{if } \alpha \text{ is odd.} \end{cases}$$
   (b) *Suppose $q \nmid k$.*
   $$c_k(q^\alpha) = \begin{cases} q^{\alpha-1}\left(\frac{-1}{q}\right)(q-1) & \text{if } q|r \text{ and } \alpha \text{ is odd} \\ -q^{\alpha-1}\left[\left(\frac{-1}{q}\right) + 1\right] & \text{if } q \nmid r \text{ and } \alpha \text{ is odd} \\ q^{\alpha-1}(q-1) & \text{if } q|r \text{ and } \alpha \text{ is even} \\ q^{\alpha-1}\left[q - 3\right] & \text{if } q \nmid r \text{ and } \alpha \text{ is even} \end{cases}$$
4. *$c_k(2^\alpha) = (-2)^\alpha$*
5. *$c_k(q^\alpha) = c_{q^{\mathrm{ord}_k(q)}}(q^\alpha)$*

Proof.

(1) We wish to show that for $(m,n) = 1$, $c_k(m)c_k(n) = c_k(mn)$. To that end, suppose $(m,n) = 1$ and $n \equiv 1 \pmod 2$. Note that $d_2(N) = d_2(2^{\mathrm{ord}_2(N)})$ for any $N \in \mathbb{N}$.

Therefore, if $d_2(1) \neq 0$ we have

$$\begin{aligned} e_2(mn) &= \frac{d_2(mn)}{d_2(1)} \\ &= \frac{d_2(2^{\mathrm{ord}_2(m)} m_1 n)}{d_2(1)} \quad \text{where } m = 2^{\mathrm{ord}_2(m)} m_1 \\ &= \frac{d_2(2^{\mathrm{ord}_2(m)})}{d_2(1)} \\ &= \frac{d_2(2^{\mathrm{ord}_2(m)})}{d_2(1)} \left(\frac{d_2(n)}{d_2(1)} \right) \\ &= \frac{d_2(m) d_2(n)}{d_2(1) d_2(1)} \\ &= e_2(m) e_2(n). \end{aligned}$$

Hence, $e_2(n)$ is multiplicative. To show $c_k(n)$ is multiplicative we follow David and Pappalardi's proof in [7, pg. 10]. Note the following two facts. First, there is a bijection between the invertible residues modulo $4n$ which are congruent to 1 modulo 4 and the invertible residues modulo n. Second, if a is congruent to 1 modulo 4, then $(r^2 - ak^2, N) = 1$ if and only if $(r^2 - ak^2, 4N) = 4$. Thus,

$$\begin{aligned} c_k(n) c_k(m) = & \sum_{\substack{a_1 \in (\mathbb{Z}/n\mathbb{Z})^* \\ (r^2 - a_1 k^2, n') = 1}} \sum_{\substack{a_2 \in (\mathbb{Z}/4m\mathbb{Z})^* \\ a_2 \equiv 1 \pmod 4 \\ (r^2 - a_2 k^2, 4m') = 4}} \left(\frac{a_1}{n} \right) e_2(n) \left(\prod_{\substack{p \mid n \\ p \neq 2}} d_p(n) \right) \\ & \cdot \left(\frac{a_2}{m} \right) e_2(m) \left(\prod_{\substack{p \mid m \\ p \neq 2}} d_p(m) \right) \end{aligned} \tag{3.29}$$

For any a_1 and a_2 in the above sums, we let a be the unique integer such that $1 \leq a \leq 4mn$, $(a, 4mn) = 1$, $a = a_1 + k_1 n = a_2 + k_2 4m$ for some integers k_1 and k_2. Then using the fact that

$$(r^2 - a_1 k^2, n) = 1 \text{ and } (r^2 - a_2 k^2, 4m) = 4 \Longleftrightarrow (r^2 - ak^2, 4mn) = 4$$

(3.29) becomes

$$\sum_{\substack{a_1\in(\mathbb{Z}/n\mathbb{Z})^*\\ a_2\in(\mathbb{Z}/4m\mathbb{Z})^*\\ a_2\equiv 1 \pmod 4\\ (r^2-ak^2,4m'n')=4}} \left(\frac{a}{n}\right) e_2(n)\prod_{\substack{p|n\\ p\neq 2}} d_p(n)\left(\frac{a}{m}\right) e_2(m)\prod_{\substack{p|m\\ p\neq 2}} d_p(m)$$

$$= \sum_{\substack{a\in(\mathbb{Z}/4mn\mathbb{Z})^*\\ a\equiv 1 \pmod 4\\ (r^2-ak^2,4m'n')=1}} \left(\frac{a}{mn}\right) e_2(mn)\prod_{\substack{p|mn\\ p\neq 2}} d_p(mn)$$

$$= c_k(mn).$$

To evaluate $c_k(q^\alpha)$ we first make the following simplification. Suppose q is an odd prime and $\alpha > 0$. Then using Lemma 3.4.2

$$c_k(q^\alpha) = \sum_{\substack{a\in(\mathbb{Z}/4q^\alpha\mathbb{Z})^*\\ a\equiv 1 \pmod 4\\ (r^2-ak^2,q^\alpha)=1}} \left(\frac{a}{q}\right)^\alpha e_2(q^\alpha)d_q(q^\alpha)$$

$$= \sum_{\substack{a\in(\mathbb{Z}/4q^\alpha\mathbb{Z})^*\\ a\equiv 1 \pmod 4\\ (r^2-ak^2,q^\alpha)=1\\ q^{\min(l_1,l_2)}|(4A^2-r^2+ak^2)}} \left(\frac{a}{q}\right)^\alpha \sum_{\substack{b\in(\mathbb{Z}/q^l\mathbb{Z})^*\\ b\equiv A \pmod{q^{l_1}}\\ 4b^2\equiv r^2-ak^2 \pmod{q^{l_2}}}} 1$$

where, as before, $l_1 = \mathrm{ord}_q(B)$, $l_2 = \mathrm{ord}_q(q^\alpha k^2) = \alpha + 2\mathrm{ord}_q(k)$ and $l = l_1 + l_2$. In Lemma 3.4.2 we computed the inner sum above and obtained

$$\sum_{\substack{b\in(\mathbb{Z}/q^l\mathbb{Z})^*\\ b\equiv A \pmod{q^{l_1}}\\ 4b^2\equiv r^2-ak^2 \pmod{q^{l_2}}}} 1 = \begin{cases} 1+\left(\frac{r^2-ak^2}{q}\right) & \text{if } q\nmid B \text{ and } (r^2-ak^2,q)=1\\ q^{\min(l_1,l_2)} & \text{if } q|B \text{ and } ak^2\equiv r^2-4A^2 \pmod{\min(l_1,l_2)}\end{cases}$$

Set $\beta = \mathrm{ord}_q(k)$. For an odd prime q and $\alpha > 0$ we have

$$c_k(q^\alpha) = c_{q^\beta}(q^\alpha) = \begin{cases} q^{\min(l_1,l_2)} \sum\limits_{\substack{a \in (\mathbb{Z}/4q^\alpha\mathbb{Z})^* \\ a \equiv 1 \pmod 4 \\ (r^2-ak^2, q^\alpha)=1 \\ ak^2 \equiv r^2 - 4A^2 \pmod{q^{\min(l_1,l_2)}}}} \left(\frac{a}{q}\right)^\alpha & \text{if } q|B \\ \sum\limits_{\substack{a \in (\mathbb{Z}/4q^\alpha\mathbb{Z})^* \\ a \equiv 1 \pmod 4 \\ (r^2-ak^2, q^\alpha)=1}} \left(\frac{a}{q}\right)^\alpha \left(1 + \left(\frac{r^2-ak^2}{q}\right)\right) & \text{if } q \nmid B \end{cases}$$

(2) Suppose $q|B$. Set $k = q^\beta k_1$, where $\mathrm{ord}_q(k) = \beta$. We consider two cases.

Case 1: If $2\beta \geq l_1$, then the condition

$$ak^2 \equiv r^2 - 4A^2 \pmod{q^{\min(l_1,l_2)}}$$

becomes

$$ak^2 \equiv r^2 - 4A^2 \pmod{q^{l_1}}$$

as $\alpha > 0$ and $l_2 = \alpha + 2\beta$. Since $k = q^\beta k_1 \Rightarrow k^2 = q^{2\beta} k_1^2$, we have

$$ak^2 \equiv r^2 - 4A^2 \pmod{q^{l_1}} \Longleftrightarrow r^2 \equiv 4A^2 \pmod{q^{l_1}}$$

Therefore,

$$c_k(q^\alpha) = q^{\min(l_1,l_2)} \sum_{\substack{a \in (\mathbb{Z}/4q^\alpha\mathbb{Z})^* \\ a \equiv 1 \pmod 4 \\ (r^2-ak^2, q^\alpha)=1 \\ ak^2 \equiv r^2 - 4A^2 \pmod{q^{l_1}}}} \left(\frac{a}{q}\right)^\alpha$$

$$= \begin{cases} q^{\min(l_1,l_2)} \sum\limits_{\substack{a \in (\mathbb{Z}/4q^\alpha\mathbb{Z})^* \\ a \equiv 1 \pmod 4 \\ (r^2-ak^2, q^\alpha)=1}} \left(\frac{a}{q}\right)^\alpha & \text{if } r^2 \equiv 4A^2 \pmod{q^{l_1}} \\ 0 & \text{otherwise} \end{cases}$$

Case 2: If $2\beta < l_1$, then

$$\begin{aligned} & ak^2 \equiv r^2 - 4A^2 \pmod{q^{\min(l_1,\alpha+2\beta)}} \\ \iff & ak_1^2 \equiv \frac{r^2-4A^2}{q^{2\beta}} \pmod{q^{\min(l_1-2\beta,\alpha)}} \quad \text{and } q^{2\beta} | (r^2-4A^2) \end{aligned}$$

Combining the two congruences

$$a \equiv 1 \pmod 4 \ ; \ ak_1^2 \equiv \frac{r^2-4A^2}{q^{2\beta}} \pmod{q^{\min(l_1-2\beta,\alpha)}}$$

we have

$$\sum_{\substack{a \in (\mathbb{Z}/4q^\alpha\mathbb{Z})^* \\ a \equiv 1 \pmod 4 \\ (r^2-ak^2, q^\alpha)=1 \\ ak_1^2 \equiv \frac{r^2-4A^2}{q^{2\beta}} \pmod{q^{\min(l_1-2\beta,\alpha)}} \\ q^{2\beta} | (r^2-4A^2)}} \left(\frac{a}{q}\right)^\alpha = \sum_{\substack{a \in (\mathbb{Z}/4q^\alpha\mathbb{Z})^* \\ (r^2-ak^2, q^\alpha)=1 \\ a \equiv \frac{r^2-4A^2}{q^{2\beta}} k_1^{-2} \pmod{4q^{\min(l_1-2\beta,\alpha)}} \\ q^{2\beta} | (r^2-4A^2)}} \left(\frac{a}{q}\right)^\alpha$$

Thus,

$$c_k(q^\alpha) = \begin{cases} q^{\alpha - \min(\alpha, l_1-2\beta)} \left(\frac{(r^2-4A^2)/q^{2\beta}}{q}\right)^\alpha & \text{if } r^2 \equiv 4A^2 \pmod{q^{2\beta}} \\ 0 & \text{otherwise.} \end{cases}$$

This concludes the proof of part (2).

For $q \nmid B$ we use Lemma 3.4.2 (see pg. 85) for the value of $d_q(q^\alpha)$.

(3a) Suppose $q \nmid B$ and $q|k$. Since $(k, 2r) = 1$, $q \nmid r$. Therefore, by Lemma 3.4.2 (2)

$$c_k(q^\alpha) = 2 \sum_{\substack{a \in (\mathbb{Z}/4q^\alpha\mathbb{Z})^* \\ a \equiv 1 \pmod 4 \\ (r^2-ak^2, q^\alpha)=1}} \left(\frac{a}{q}\right)^\alpha = 2 \sum_{\substack{a \in (\mathbb{Z}/4q^\alpha\mathbb{Z})^* \\ a \equiv 1 \pmod 4}} \left(\frac{a}{q}\right)^\alpha = \begin{cases} 2\phi(q^\alpha) & \text{if } \alpha \text{ is even} \\ 0 & \text{if } \alpha \text{ is odd} \end{cases}$$

(3b) Suppose $q \nmid B$ and $q \nmid k$. First, consider odd α. Then using Lemma 3.4.2 (2)

$$
\begin{aligned}
c_k(q^\alpha) = & \sum_{\substack{a \in (\mathbb{Z}/4q^\alpha\mathbb{Z})^* \\ a \equiv 1 \pmod 4 \\ (r^2 - ak^2, q^\alpha) = 1}} \left(\frac{a}{q}\right)^\alpha \left(1 + \left(\frac{r^2 - ak^2}{q}\right)\right) \\
= & \sum_{\substack{a \in (\mathbb{Z}/4q^\alpha\mathbb{Z})^* \\ a \equiv 1 \pmod 4 \\ (r^2 - ak^2, q^\alpha) = 1}} \left[\left(\frac{a}{q}\right) + \left(\frac{a}{q}\right)\left(\frac{r^2 - ak^2}{q}\right)\right] \\
= & \, q^{\alpha-1} \sum_{\substack{a \in (\mathbb{Z}/q\mathbb{Z})^* \\ r^2 \not\equiv ak^2 \pmod q}} \left[\left(\frac{a}{q}\right) + \left(\frac{a}{q}\right)\left(\frac{r^2 - ak^2}{q}\right)\right] \\
= & \, q^{\alpha-1}\left[\sum_{\substack{a \in (\mathbb{Z}/q\mathbb{Z})^* \\ r^2 \not\equiv ak^2 \pmod q}} \left(\frac{a}{q}\right) + \sum_{a \in (\mathbb{Z}/q\mathbb{Z})^*} \left(\frac{a}{q}\right)\left(\frac{r^2 - ak^2}{q}\right)\right] \\
= & \, q^{\alpha-1}\left[-\left(\frac{r^2k^{-2}}{q}\right) + \sum_{a \in (\mathbb{Z}/q\mathbb{Z})^*} \left(\frac{a^{-1}}{q}\right)\left(\frac{r^2 - ak^2}{q}\right)\right] \\
= & \, q^{\alpha-1}\left[-\left(\frac{r^2}{q}\right) + \sum_{a \in (\mathbb{Z}/q\mathbb{Z})^*} \left(\frac{a^{-1}r^2 - k^2}{q}\right)\right] \\
= & \begin{cases} q^{\alpha-1}\left(\frac{-1}{q}\right)(q-1) & \text{if } q | r \\ q^{\alpha-1}\left[-1 - \left(\frac{-1}{q}\right)\right] & \text{if } q \nmid r \end{cases}
\end{aligned}
$$

If α is even, then

$$\begin{aligned}
c_k(q^\alpha) = & \sum_{\substack{a\in(\mathbb{Z}/4q^\alpha\mathbb{Z})^* \\ a\equiv 1 \pmod 4 \\ (r^2-ak^2,q^\alpha)=1}} \left(\frac{a}{q}\right)^\alpha \left(1+\left(\frac{r^2-ak^2}{q}\right)\right) \\
= & \sum_{\substack{a\in(\mathbb{Z}/4q^\alpha\mathbb{Z})^* \\ a\equiv 1 \pmod 4 \\ (r^2-ak^2,q^\alpha)=1}} 1 + q^{\alpha-1} \sum_{\substack{a\in(\mathbb{Z}/q\mathbb{Z})^* \\ (r^2-ak^2,q^\alpha)=1}} \left(\frac{r^2-ak^2}{q}\right) \\
= & \, q^{\alpha-1} \sum_{\substack{a\in(\mathbb{Z}/q\mathbb{Z})^* \\ a\not\equiv r^2k^{-2} \pmod q}} 1 \\
& + q^{\alpha-1}\left[\sum_{\substack{a\in(\mathbb{Z}/q\mathbb{Z})^* \\ a\not\equiv r^2k^{-2} \pmod q}} \left(\frac{r^2-ak^2}{q}\right) + \left(\frac{r^2}{q}\right) - \left(\frac{r^2}{q}\right)\right] \\
= & \begin{cases} q^{\alpha-1}[q-2] - q^{\alpha-1} & \text{if } q \nmid r \\ q^{\alpha-1}[q-1] & \text{if } q|r \end{cases}
\end{aligned}$$

(4) Throughout the proof of part (4) we will be using parts (4)-(6) of Lemma 3.4.2 from page 85. Note that by definition

$$d_2(1) = \sum_{\substack{b\in(\mathbb{Z}/2^{2+\mathrm{ord}_2(B)})^* \\ b\equiv A \pmod{2^{\mathrm{ord}_2(B)}} \\ 4b^2\equiv r^2-ak^2 \pmod{2^2}}} 1$$

therefore

$$d_2(1) = \begin{cases} 2 & \text{if } 2\nmid B \text{ and } a\equiv 1 \pmod 4 \\ 4 & \text{if } 2|B \text{ and } a\equiv 1 \pmod 4 \\ 0 & \text{otherwise.} \end{cases}$$

Set $l_2 = \mathrm{ord}_2(4\cdot 2^\alpha k^2) = \alpha+2$; $l_1 = \mathrm{ord}_2(B)$; $l = \mathrm{ord}_2(4B2^\alpha k^2) = \alpha+2+l_1$. Suppose $l_1 = 0$. Note that since r and k are odd

$$r^2-ak^2 \equiv 4 \pmod{2^{\min(5,\alpha+2)}} \Rightarrow a\equiv 5 \pmod 8 \Rightarrow \left(\frac{a}{2}\right) = \left(\frac{2}{a}\right) = -1.$$

Using Lemma 3.4.2 (4) with $l_1 = 0$ we have

$$\begin{aligned} c_k(2^\alpha) &= \sum_{a \in (\mathbb{Z}/2^{\alpha+2}\mathbb{Z})^*} \left(\frac{a}{2}\right)^\alpha \frac{d_2(2^\alpha)}{d_2(1)} \\ &= \sum_{\substack{a \in (\mathbb{Z}/2^{\alpha+2}\mathbb{Z})^* \\ r^2 - ak^2 \equiv 4 \pmod{2^{\min(5,\alpha+2)}}}} \left(\frac{a}{2}\right)^\alpha \frac{2^{\min(4,\alpha+1)}}{2} \\ &= \sum_{\substack{a \in (\mathbb{Z}/2^{\alpha+2}\mathbb{Z})^* \\ r^2 - ak^2 \equiv 4 \pmod{2^{\min(5,\alpha+2)}}}} (-1)^\alpha \frac{2^{\min(4,\alpha+1)}}{2} \end{aligned}$$

If $\alpha = 1$, then

$$c_k(2) = \sum_{\substack{a \in (\mathbb{Z}/2^3\mathbb{Z})^* \\ r^2 - ak^2 \equiv 4 \pmod 8}} \left(\frac{a}{2}\right) \frac{2^2}{2} = \sum_{\substack{a \in (\mathbb{Z}/2^3\mathbb{Z})^* \\ a \equiv 5 \pmod 8}} \left(\frac{a}{2}\right) 2 = -2$$

If $\alpha = 2$, then

$$c_k(2^2) = \sum_{\substack{a \in (\mathbb{Z}/2^4\mathbb{Z})^* \\ r^2 - ak^2 \equiv 4 \pmod{2^4}}} \left(\frac{a}{2}\right)^2 \frac{2^3}{2} = 2^2$$

If $\alpha \geq 3$, then

$$c_k(2^\alpha) = \sum_{\substack{a \in (\mathbb{Z}/2^{\alpha+2}\mathbb{Z})^* \\ r^2 - ak^2 \equiv 4 \pmod{2^5}}} \left(\frac{a}{2}\right)^\alpha \frac{2^4}{2} = 2^3 \cdot 2^{\alpha-3}(-1)^\alpha = (-2)^\alpha$$

Suppose $l_1 > 0$, we have three cases.

Case 1: $l_1 = 1$

Using Lemma 3.4.2 (4) $c_k(q^\alpha)$ is

$$c_k(2^\alpha) = \sum_{\substack{a \in (\mathbb{Z}/2^{\alpha+2}\mathbb{Z})^* \\ 4 \equiv r^2 - ak^2 \pmod{2^{\min(5,l_2)}}}} \left(\frac{a}{2}\right)^\alpha \frac{2^{\min(5,l_2)}}{4}.$$

If $\alpha = 1$, then

$$c_k(2) = \sum_{\substack{a \in (\mathbb{Z}/2^3\mathbb{Z})^* \\ 4 \equiv r^2 - ak^2 \pmod{2^{\min(5,3)}}}} \left(\frac{a}{2}\right) \frac{2^{\min(5,3)}}{4} = \sum_{\substack{a \in (\mathbb{Z}/2^3\mathbb{Z})^* \\ 4 \equiv r^2 - ak^2 \pmod{2^3}}} (-2) = -2.$$

If $\alpha = 2$, then

$$c_k(2^2) = \sum_{\substack{a \in (\mathbb{Z}/2^4\mathbb{Z})^* \\ 4 \equiv r^2 - ak^2 \pmod{2^4}}} \left(\frac{a}{2}\right)^2 \frac{2^4}{4} = 2^2.$$

If $\alpha \geq 3$, then

$$c_k(2^\alpha) = \sum_{\substack{a \in (\mathbb{Z}/2^{\alpha+2}\mathbb{Z})^* \\ 4 \equiv r^2 - ak^2 \pmod{2^5}}} \left(\frac{a}{2}\right)^\alpha \frac{2^5}{4} = (-1)^\alpha \cdot 2^3 \cdot 2^{\alpha+2-5} = (-2)^\alpha.$$

Case 2: $l_1 \geq 2$ and $l_2 \leq l_1 + 3$

Using Lemma 3.4.2 (5)

$$c_k(2^\alpha) = \sum_{\substack{a \in (\mathbb{Z}/2^{\alpha+2}\mathbb{Z})^* \\ 4A^2 \equiv r^2 - ak^2 \pmod{2^{l-l_1}}}} \left(\frac{a}{2}\right)^\alpha \frac{2^{l-l_1}}{4} = \frac{2^{\alpha+2}}{4}(-1)^\alpha \sum_{\substack{a \in (\mathbb{Z}/2^{\alpha+2}\mathbb{Z})^* \\ 4A^2 \equiv r^2 - ak^2 \pmod{2^{\alpha+2}}}} 1 = (-2)^\alpha.$$

Case 3: $l_1 \geq 2$ and $l_2 \geq l_1 + 4$

Using Lemma 3.4.2 (6)

$$\begin{aligned} c_k(2^\alpha) &= \sum_{\substack{a \in (\mathbb{Z}/2^{\alpha+2}\mathbb{Z})^* \\ 4A^2 \equiv r^2 - ak^2 \pmod{2^{l_1+3}}}} \left(\frac{a}{2}\right)^\alpha \frac{2^{l_1+3}}{4} \\ &= (-1)^\alpha \frac{2^{l_1+3}}{4} \sum_{\substack{a \in (\mathbb{Z}/2^{\alpha+2}\mathbb{Z})^* \\ 4A^2 \equiv r^2 - ak^2 \pmod{2^{l_1+3}}}} 1 \\ &= (-1)^\alpha \cdot 2^{l_1+1} \cdot 2^{\alpha+2-(l_1+3)} = (-2)^\alpha. \end{aligned}$$

□

3.7 Computing the Constant

Let $r, A, B \in \mathbb{Z}$ with $(A, B) = 1$ and r odd. Recall the definition of $C_{r,A,B}$

$$C_{r,A,B} = \sum_{\substack{k \in \mathbb{N} \\ (k,2r)=1}} \frac{1}{k} \sum_{n=1}^{\infty} \frac{1}{n\phi(4nBk^2)} \sum_{a \in (\mathbb{Z}/4n\mathbb{Z})^*} \left(\frac{a}{n}\right) C_r(a, n, k)$$

where as before (see pg. 84)

$$C_r(a,n,k) = \prod_{\substack{p|(4Bnk^2)\\ p \text{ prime}}} d_p(n)$$

and

$$d_p(n) = \sum_{\substack{b\in(\mathbb{Z}/p^{\mathrm{ord}_p(4Bnk^2)}\mathbb{Z})^*\\ b\equiv A \pmod{p^{\mathrm{ord}_p(B)}}\\ 4b^2\equiv r^2-ak^2 \pmod{p^{\mathrm{ord}_p(4nk^2)}}}} 1.$$

In this section we show that

$$\begin{aligned} C_{r,A,B} &= c_{r,A,B} \\ &\cdot \prod_{\substack{q,\text{odd}\\ q|B\\ q|r}} \left(1 + \frac{\left(\frac{-1}{q}\right) - \left(\frac{-1}{q}\right)^{\mathrm{ord}_q(B)+1} q^{-2\mathrm{ord}_q(B)}}{q^2 - \left(\frac{-1}{q}\right)} + \frac{\left(\frac{-1}{q}\right)^{\mathrm{ord}_q(B)+1}}{q^{2\mathrm{ord}_q(B)}\left(q - \left(\frac{-1}{q}\right)\right)}\right) \\ &\cdot \frac{2}{3\phi(B)} \prod_{\substack{q,\text{odd}\\ q\nmid B\\ q|r}} \left(\frac{q}{q - \left(\frac{-1}{q}\right)}\right) \prod_{\substack{q,\text{odd}\\ q\nmid B\\ q\nmid r}} \left(1 - \frac{\left(\frac{-1}{q}\right)q - 1}{(q-1)(q^2-1)}\right). \end{aligned}$$

First, we record several evaluations of d_p which follow directly from Lemma 3.4.2 (see pg. 85).

Lemma 3.7.1. *Suppose $p \nmid 2n$,*

1. *If $p|B$ and $p \nmid k$, then $d_p(1) = d_p(n) = 1$*
2. *Suppose $p|k$.*
   (a) *If $p|B$, then*

$$\begin{aligned} d_p(1) &= d_p(n) \\ &= \begin{cases} p^{\min(\mathrm{ord}_p(B),\mathrm{ord}_p(4nk^2))} & \text{if } 4A^2 \equiv r^2 \pmod{p^{\min(\mathrm{ord}_p(B),\mathrm{ord}_p(4nk^2))}} \\ 0 & \text{otherwise} \end{cases} \end{aligned}$$

   (b) *If $p \nmid B$ and $(r^2 - ak^2, p) = 1$, then $d_p(1) = d_p(n) = 2$*

Proof.

(1) By Lemma 3.4.2 (1).

(2a) By Lemma 3.4.2 (1) and (3).

(2b) By Lemma 3.4.2 (2).

□

If $a \equiv 3 \pmod 4$ or $(r^2 - ak^2, n') \neq 1$, then $C_r(a, n, k) = 0$. Therefore, we may write

$$\begin{aligned} C_{r,A,B} &= \sum_{\substack{k\in\mathbb{N}\\(k,2r)=1}} \frac{1}{k}\sum_{n=1}^{\infty} \frac{1}{n\phi(4Bnk^2)} \sum_{\substack{a\in(\mathbb{Z}/4n\mathbb{Z})^*\\a\equiv 1 \pmod 4\\(r^2-ak^2,n')=1}} \left(\frac{a}{n}\right) \prod_{\substack{p,\text{prime}\\p|4Bnk^2}} d_p(n) \\ &= \sum_{\substack{k\in\mathbb{N}\\(k,2r)=1}} \frac{1}{k}\sum_{n=1}^{\infty} \frac{1}{n\phi(4Bnk^2)} \sum_{\substack{a\in(\mathbb{Z}/4n\mathbb{Z})^*\\a\equiv 1 \pmod 4\\(r^2-ak^2,n')=1}} \left(\frac{a}{n}\right) \\ &\quad \cdot d_2(n) \left(\prod_{\substack{p|n\\p\neq 2}} d_p(n)\right) \left(\prod_{\substack{p|k\\p\nmid 2n}} d_p(n)\right) \left(\prod_{\substack{p|B\\p\nmid 2nk}} d_p(n)\right) \end{aligned}$$

If $p|B$ and $p \nmid 2nk$, Lemma 3.7.1 (1) implies that $d_p(n) = 1$. Therefore, $C_{r,A,B}$ simplifies to

$$\begin{aligned} C_{r,A,B} = &\sum_{\substack{k\in\mathbb{N}\\(k,2r)=1}} \frac{1}{k}\sum_{n=1}^{\infty} \frac{1}{n\phi(4Bnk^2)} \\ &\cdot \sum_{\substack{a\in(\mathbb{Z}/4n\mathbb{Z})^*\\a\equiv 1 \pmod 4\\(r^2-ak^2,n')=1}} \left(\frac{a}{n}\right) d_2(n) \left(\prod_{\substack{p|n\\p\neq 2}} d_p(n)\right) \left(\prod_{\substack{p|k\\p\nmid 2n}} d_p(n)\right) \end{aligned}$$

For a prime p such that $p|k$ and $p \nmid 2n$ Lemma 3.7.1 (2) gives $d_p(n) = d_p(1)$. Therefore, we write $C_{r,A,B}$ as

$$C_{r,A,B} = \sum_{\substack{k\in\mathbb{N}\\(k,2r)=1}} \frac{1}{k}\sum_{n=1}^{\infty} \frac{1}{n\phi(4Bnk^2)} \cdot \sum_{\substack{a\in(\mathbb{Z}/4n\mathbb{Z})^*\\a\equiv 1 \pmod 4\\(r^2-ak^2,n')=1}} \left(\frac{a}{n}\right) d_2(n) \left(\prod_{\substack{p|n\\p\neq 2}} d_p(n)\right)\left(\prod_{\substack{p|k\\p\nmid 2n}} d_p(1)\right).$$

By definition,

$$d_2(1) = \sum_{\substack{b\in(\mathbb{Z}/2^{\mathrm{ord}_2(4Bk^2)}\mathbb{Z})^*\\b\equiv A \pmod{2^{\mathrm{ord}_2(B)}}\\4b^2\equiv r^2-ak^2 \pmod{2^{\mathrm{ord}_2(4k^2)}}}} 1$$

and

$$d_2(n) = \sum_{\substack{b\in(\mathbb{Z}/2^{\mathrm{ord}_2(4Bnk^2)}\mathbb{Z})^*\\b\equiv A \pmod{2^{\mathrm{ord}_2(B)}}\\4b^2\equiv r^2-ak^2 \pmod{2^{\mathrm{ord}_2(4nk^2)}}}} 1.$$

If $d_2(1) = 0$, then $4A^2 \not\equiv r^2 - ak^2 \pmod{2^{\min(\mathrm{ord}_2(B),\mathrm{ord}_2(4k^2))}}$. Since $\min(\mathrm{ord}_2(B), \mathrm{ord}_2(4k^2)) \leq \min(\mathrm{ord}_2(B), \mathrm{ord}_2(4nk^2))$, we also have that $4A^2 \not\equiv r^2 - ak^2 \pmod{2^{\min(\mathrm{ord}_2(B),\mathrm{ord}_2(4nk^2))}}$. Therefore, $d_2(n) = 0$. Recall our definition of $e_2(n)$

$$e_2(n) = \begin{cases} \frac{d_2(n)}{d_2(1)} & \text{if } d_2(1) \neq 0 \\ 0 & \text{if } d_2(1) = 0. \end{cases}$$

Thus, $d_2(n) = d_2(1)e_2(n)$ and $C_{r,A,B}$ becomes

$$C_{r,A,B} = \sum_{\substack{k\in\mathbb{N}\\(k,2r)=1}} \frac{1}{k}\sum_{n=1}^{\infty} \frac{1}{n\phi(4Bnk^2)} \cdot \sum_{\substack{a\in(\mathbb{Z}/4n\mathbb{Z})^*\\a\equiv 1 \pmod 4\\(r^2-ak^2,n')=1}} \left(\frac{a}{n}\right) d_2(1)e_2(n) \left(\prod_{\substack{p|n\\p\neq 2}} d_p(n)\right)\left(\prod_{\substack{p|k\\p\nmid 2n}} d_p(1)\right).$$

Suppose p is an odd prime, recall

$$d_p(1) := \sum_{\substack{b\in(\mathbb{Z}/p^{\mathrm{ord}_p(4Bk^2)}\mathbb{Z})^* \\ b\equiv A \pmod{p^{\mathrm{ord}_p(B)}} \\ 4b^2\equiv r^2-ak^2 \pmod{p^{\mathrm{ord}_p(4k^2)}}}} .$$

Since p is an odd prime $\mathrm{ord}_p(4k^2) = \mathrm{ord}_p(k^2)$ and our last condition on the sum in the definition of $d_p(1)$ becomes $4b^2 \equiv r^2 \pmod{p^{\mathrm{ord}_p(4k^2)}}$. We have shown that for odd primes p $d_p(1)$ does not depend on a. Therefore, we write

$$C_{r,A,B} = \sum_{\substack{k\in\mathbb{N} \\ (k,2r)=1}} \frac{1}{k}\sum_{n=1}^{\infty} \frac{1}{n\phi(4Bnk^2)} \left(\prod_{\substack{p|k \\ p\nmid 2n}} d_p(1)\right) \cdot \sum_{\substack{a\in(\mathbb{Z}/4n\mathbb{Z})^* \\ a\equiv 1 \pmod 4 \\ (r^2-ak^2,n')=1}} \left(\frac{a}{n}\right) d_2(1)e_2(n)\prod_{\substack{p|n \\ p\neq 2}} d_p(n).$$

Since $a \equiv 1 \pmod 4$, $d_2(1)$ *only* depends on B modulo 2 and our definition of $c_k(n)$ is

$$c_k(n) = \sum_{\substack{a\in(\mathbb{Z}/4n\mathbb{Z})^* \\ a\equiv 1 \pmod 4 \\ (r^2-ak^2,n')=1}} \left(\frac{a}{n}\right) e_2(n)\prod_{\substack{p|n \\ p\neq 2}} d_p(n).$$

We write $C_{r,A,B}$ as

$$\begin{aligned} C_{r,A,B} &= d_2(1) \sum_{\substack{k\in\mathbb{N} \\ (k,2r)=1}} \frac{1}{k}\sum_{n=1}^{\infty} \frac{1}{n\phi(4Bnk^2)} \left(\prod_{\substack{p|k \\ p\nmid 2n}} d_p(1)\right) c_k(n) \\ &= d_2(1) \sum_{\substack{k\in\mathbb{N} \\ (k,2r)=1}} \frac{1}{k}\sum_{n=1}^{\infty} \frac{1}{n\phi(4Bnk^2)} \left(\prod_{\substack{p|(B,k) \\ p\nmid 2n}} d_p(1)\right) \left(\prod_{\substack{p|k \\ p\nmid 2Bn}} d_p(1)\right) c_k(n). \end{aligned}$$

For integers x and y denote by $\nu(x,y)$ the number of distinct prime divisors of the $gcd(x,y)$. Using Lemma 3.7.1

$$\prod_{\substack{p|k \\ p\nmid 2Bn}} d_p(1) = 2^{\nu(k)-\nu(k,2Bn)}.$$

Recall

$$\phi(AB) = \phi(A)\phi(B)\frac{(A,B)}{\phi((A,B))} \tag{3.30}$$

where (A,B) is the greatest common divisor of A and B. So, we can write

$$\begin{aligned} C_{r,A,B} = d_2(1) & \sum_{\substack{k\in\mathbb{N} \\ (k,2r)=1}} \frac{2^{\nu(k)}}{k\phi(4Bk^2)} \\ & \cdot \sum_{n\in\mathbb{N}} \frac{\left[\prod_{\substack{p|(B,k) \\ p\nmid 2n}} d_p(1)\right] \phi((n,4Bk^2))}{n\phi(n)(n,4Bk^2)2^{\nu(k,2Bn)}} c_k(n) \end{aligned} \tag{3.31}$$

For positive integers x, y, and z we have the identities:

1.
$$(x,(y,z)) = (x,y,z) \tag{3.32}$$

2.
$$(x,yz) = (x,y)\left(\frac{x}{(x,y)},z\right). \tag{3.33}$$

Identity (3.33) along with the fact that ν is additive and k is odd implies that

$$\begin{aligned} 2^{\nu(k,2Bn)} &= 2^{\nu\left((k,B)\cdot\left(\frac{k}{(k,B)},n\right)\right)} \\ &= 2^{\nu(k,B)+\nu\left(\frac{k}{(k,B)},n\right)-\nu\left((k,B),\left(\frac{k}{(k,B)},n\right)\right)} \end{aligned} \tag{3.34}$$

Observe that

$$\begin{aligned} \left((k,B),\left(\frac{k}{(k,B)},n\right)\right) &= \left(\left(B,\left(k,\frac{k}{(k,B)}\right)\right),n\right) && \text{by (3.32)} \\ &= \left(\left(B,\frac{k}{(k,B)}\right),n\right) && \text{by (3.33)} \\ &= \left(\frac{(k,B^2)}{(k,B)},n\right) && \text{by (3.33).} \end{aligned}$$

Thus, (3.34) becomes

$$2^{\nu(k,2Bn)} = \frac{2^{\nu(k,B)} \cdot 2^{\nu\left(\frac{k}{(k,B)},n\right)}}{2^{\nu\left(\frac{(k,B^2)}{(k,B)},n\right)}}. \tag{3.35}$$

Using (3.35) we may write (3.31) as

$$\begin{aligned} C_{r,A,B} = d_2(1) \sum_{\substack{k\in\mathbb{N}\\(k,2r)=1}} \frac{2^{\nu(k)}}{k2^{\nu(k,B)}\phi(4Bk^2)} \\ \cdot \sum_{n\in\mathbb{N}} \frac{\left[\prod_{\substack{p|(B,k)\\p\nmid 2n}} d_p(1)\right] \phi((n,4Bk^2))2^{\nu\left(\frac{(k,B^2)}{(k,B)},n\right)}}{n\phi(n)(n,4Bk^2)2^{\nu\left(\frac{k}{(k,B)},n\right)}} c_k(n). \end{aligned} \tag{3.36}$$

In order to make the inner sum multiplicative in n, we require the following lemma.

Lemma 3.7.2. *Suppose $p|(B,n,k)$. If $d_p(1) = 0$, then $c_k(n) = 0$.*

Proof.

Let $\alpha = \mathrm{ord}_p(B)$ and $\beta = \mathrm{ord}_p(k)$. By definition

$$d_p(1) = \sum_{\substack{b\in(\mathbb{Z}/p^{\alpha+2\beta}\mathbb{Z})^*\\ b\equiv A \pmod{p^\alpha}\\ 4b^2\equiv r^2-ak^2 \pmod{p^{2\beta}}}} 1$$

and

$$d_p(n) = \sum_{\substack{b\in(\mathbb{Z}/p^{\alpha+2\beta+\mathrm{ord}_p(n)}\mathbb{Z})^*\\ b\equiv A \pmod{p^\alpha}\\ 4b^2\equiv r^2-ak^2 \pmod{p^{2\beta+\mathrm{ord}_p(n)}}}} 1$$

Recall from page 121 that $d_p(1)$ does not depend on a. Therefore, for any a one can see that if $d_p(1) = 0$, then $4A^2 \not\equiv r^2 - ak^2 \pmod{p^{\min(\alpha,2\beta)}}$. Since $\min(\alpha, 2\beta) \leq \min(\alpha, 2\beta + \mathrm{ord}_p(n))$,

$$\begin{aligned} 4A^2 \not\equiv r^2 - ak^2 \pmod{p^{\min(\alpha,2\beta)}} &\Rightarrow 4A^2 \not\equiv r^2 - ak^2 \pmod{p^{\min(\alpha,2\beta+\mathrm{ord}_p(n))}} \\ &\Rightarrow d_p(n) = 0 \end{aligned}$$

So, if $d_p(1) = 0$, then $d_p(n) = 0$ for all a. Thus, $c_k(n) = 0$.

□

For $p|(B,k,n)$, define

$$f_p = \begin{cases} d_p(1) & \text{if } d_p(1) \neq 0 \\ 1 & \text{if } d_p(1) = 0. \end{cases}$$

Then by Lemma 3.7.2,

$$\left(\prod_{\substack{p|(B,k) \\ p\nmid 2n}} d_p(1) \right) c_k(n) = \frac{\prod_{p|(B,k)} d_p(1)}{\prod_{p|(B,k,n)} f_p} c_k(n)$$

Note that if $d_p(1) = 0$ for some $p|(B,k)$, then both sides of the above equation are 0. Using Lemma 3.7.2, we write $C_{r,A,B}$ as

$$\begin{aligned} C_{r,A,B} = d_2(1) \sum_{\substack{k\in\mathbb{N} \\ (k,2r)=1}} & \frac{2^{\nu(k)} \left[\prod_{p|(B,k)} d_p(1)\right]}{k 2^{\nu(k,B)} \phi(4Bk^2)} \\ & \cdot \sum_{n\in\mathbb{N}} \frac{\phi((n,4Bk^2)) 2^{\nu\left(\frac{(k,B^2)}{(k,B)},n\right)}}{\left[\prod_{p|(B,k,n)} f_p\right] n\phi(n)(n,4Bk^2) 2^{\nu\left(\frac{k}{(k,B)},n\right)}} c_k(n). \end{aligned}$$

Another application of (3.30) yields

$$\begin{aligned} C_{r,A,B} = \frac{d_2(1)}{\phi(4B)} \sum_{\substack{k\in\mathbb{N} \\ (k,2r)=1}} & \frac{2^{\nu(k)} \left[\prod_{p|(B,k)} d_p(1)\right] \phi((4B,k^2))}{k 2^{\nu(k,B)} \phi(k^2)(4B,k^2)} \\ & \cdot \sum_{n\in\mathbb{N}} \frac{\phi((n,4Bk^2)) 2^{\nu\left(\frac{(k,B^2)}{(k,B)},n\right)}}{\left[\prod_{p|(B,k,n)} f_p\right] n\phi(n)(n,4Bk^2) 2^{\nu\left(\frac{k}{(k,B)},n\right)}} c_k(n). \end{aligned} \tag{3.37}$$

Due to the multiplicativity of the functions in the inner sum above we may rewrite the inner sum as

$$\prod_{q,\ \text{prime}} \sum_{\alpha\geq 0} \frac{\phi((q^\alpha,4Bk^2)) 2^{\nu\left(\frac{(k,B^2)}{(k,B)},q^\alpha\right)}}{\left[\prod_{p|(B,k,q^\alpha)} f_p\right] q^\alpha \phi(q^\alpha)(q^\alpha,4Bk^2) 2^{\nu\left(\frac{k}{(k,B)},q^\alpha\right)}} c_k(q^\alpha). \tag{3.38}$$

Since $c_k(q^\alpha) = c_{q^{\mathrm{ord}_q(k)}}(q^\alpha)$, the product above may be written as

$$\begin{aligned}
&\prod_{q\nmid k}\left(\sum_{\alpha\geq 0}\frac{\phi((q^\alpha,4B))}{q^\alpha\phi(q^\alpha)(q^\alpha,4B)}c_1(q^\alpha)\right)\\
&\cdot\prod_{q|k}\left(\sum_{\alpha\geq 0}\frac{\phi((q^\alpha,4Bk^2))2^{\nu\left(\frac{(k,B^2)}{(k,B)},q^\alpha\right)}}{\left[\prod_{p|(B,k,q^\alpha)}f_p\right]q^\alpha\phi(q^\alpha)(q^\alpha,4Bk^2)2^{\nu\left(\frac{k}{(k,B)},q^\alpha\right)}}c_{q^{\mathrm{ord}_q(k)}}(q^\alpha)\right)\\
&=\prod_{q,\text{prime}}\left(\sum_{\alpha\geq 0}\frac{\phi((q^\alpha,4B))}{q^\alpha\phi(q^\alpha)(q^\alpha,4B)}c_1(q^\alpha)\right)\\
&\cdot\prod_{q|k}\frac{\left(\sum_{\alpha\geq 0}\frac{\phi((q^\alpha,4Bk^2))2^{\nu\left(\frac{(k,B^2)}{(k,B)},q^\alpha\right)}}{\left[\prod_{p|(B,k,q^\alpha)}f_p\right]q^\alpha\phi(q^\alpha)(q^\alpha,4Bk^2)2^{\nu\left(\frac{k}{(k,B)},q^\alpha\right)}}c_{q^{\mathrm{ord}_q(k)}}(q^\alpha)\right)}{\left(\sum_{\alpha\geq 0}\frac{\phi((q^\alpha,4B))}{q^\alpha\phi(q^\alpha)(q^\alpha,4B)}c_1(q^\alpha)\right)}
\end{aligned}\tag{3.39}$$

Substituting (3.39) into (3.37) we obtain

$$\begin{aligned}
C_{r,A,B}=\frac{d_2(1)}{\phi(4B)}&\prod_{q}\left(\sum_{\alpha\geq 0}\frac{\phi((q^\alpha,4B))c_1(q^\alpha)}{q^\alpha\phi(q^\alpha)(q^\alpha,4B)}\right)\\
&\cdot\sum_{\substack{k\in\mathbb{N}\\(k,2r)=1}}\left(\frac{2^{\nu(k)}\left[\prod_{p|(B,k)}d_p(1)\right]\phi((4B,k^2))}{k2^{\nu(k,B)}\phi(k^2)(4B,k^2)}\right)\\
&\cdot\prod_{\substack{q^\beta||k\\\beta\geq 1}}\frac{\left(\sum_{\alpha\geq 0}\frac{\phi((q^\alpha,4Bq^{2\beta}))2^{\nu\left(\frac{(q^\beta,B^2)}{(q^\beta,B)},q^\alpha\right)}c_{q^\beta}(q^\alpha)}{\left[\prod_{p|(B,q)}f_p\right]q^\alpha\phi(q^\alpha)(q^\alpha,4Bq^{2\beta})2^{\nu\left(\frac{q^\beta}{(q^\beta,B)},q^\alpha\right)}}\right)}{\left(\sum_{\alpha\geq 0}\frac{\phi((q^\alpha,4B))c_1(q^\alpha)}{q^\alpha\phi(q^\alpha)(q^\alpha,4B)}\right)}
\end{aligned}\tag{3.40}$$

Again we have a sum of multiplicative functions which allows us to write the inner sum as

$$\begin{aligned}
\prod_{\substack{q\\q\nmid 2r}}\Bigg[1+\sum_{\beta\geq 1}&\left(\frac{\frac{2^{\nu(q^\beta)}\left[\prod_{p|(B,q)}d_p(1)\right]\phi((4B,q^{2\beta}))}{q^\beta 2^{\nu(q^\beta,B)}\phi(q^{2\beta})(4B,q^{2\beta})}}{\sum_{\alpha\geq 0}\frac{\phi((q^\alpha,4B))c_1(q^\alpha)}{q^\alpha\phi(q^\alpha)(q^\alpha,4B)}}\right)\\
&\cdot\left(\sum_{\alpha\geq 0}\frac{\phi((q^\alpha,4Bq^{2\beta}))2^{\nu\left(\frac{(q^\beta,B^2)}{(q^\beta,B)},q^\alpha\right)}c_{q^\beta}(q^\alpha)}{\left[\prod_{p|(B,q)}f_p\right]q^\alpha\phi(q^\alpha)(q^\alpha,4Bq^{2\beta})2^{\nu\left(\frac{q^\beta}{(q^\beta,B)},q^\alpha\right)}}\right)\Bigg]
\end{aligned}\tag{3.41}$$

Putting (3.41) into (3.40) yields

$$
\begin{aligned}
C_{r,A,B} = \frac{d_2(1)}{\phi(4B)} \cdot & \left(1 + \sum_{\alpha \geq 1} \frac{\phi((2^\alpha, 4B))c_1(2^\alpha)}{2^\alpha \phi(2^\alpha)(2^\alpha, 4B)}\right) \\
& \cdot \prod_{\substack{q,\text{odd} \\ q \nmid B \\ q \mid r}} \left(\sum_{\alpha \geq 0} \frac{c_1(q^\alpha)}{q^\alpha \phi(q^\alpha)}\right) \\
& \cdot \prod_{\substack{q,\text{odd} \\ q \nmid B \\ q \nmid r}} \left(\sum_{\alpha \geq 0} \frac{c_1(q^\alpha)}{q^\alpha \phi(q^\alpha)} + \sum_{\beta \geq 1} \frac{2}{q^\beta \phi(q^{2\beta})} \sum_{\alpha \geq 0} \frac{\phi((q^\alpha, q^{2\beta}))c_{q^\beta}(q^\alpha)}{q^\alpha \phi(q^\alpha)(q^\alpha, q^{2\beta}) 2^{\nu(q^\beta, q^\alpha)}}\right) \\
& \cdot \prod_{\substack{q,\text{odd} \\ q \mid B \\ q \mid r}} \left(1 + \sum_{\alpha \geq 1} \frac{\phi((q^\alpha, B))c_1(q^\alpha)}{q^\alpha \phi(q^\alpha)(q^\alpha, B)}\right) \\
& \cdot \prod_{\substack{q,\text{odd} \\ q \mid B \\ q \nmid r}} \left(1 + \sum_{\alpha \geq 1} \frac{\phi((q^\alpha, B))c_1(q^\alpha)}{q^\alpha \phi(q^\alpha)(q^\alpha, B)}\right. \\
& \quad \left. + \frac{d_q(1)}{f_q} \sum_{\beta \geq 1} \frac{\phi((B, q^{2\beta}))}{q^\beta \phi(q^{2\beta})(B, q^{2\beta})} \sum_{\alpha \geq 0} \frac{\phi((q^\alpha, Bq^{2\beta}))2^{\nu\left(\frac{(q^\beta, B^2)}{(q^\beta, B)}, q^\alpha\right)} c_{q^\beta}(q^\alpha)}{q^\alpha \phi(q^\alpha)(q^\alpha, 4Bq^{2\beta})2^{\nu\left(\frac{q^\beta}{(q^\beta, B)}, q^\alpha\right)}}\right)
\end{aligned}
\tag{3.42}
$$

Define $C(2)$ as

$$C(2) = 1 + \sum_{\alpha \geq 1} \frac{\phi((2^\alpha, 4B))c_1(2^\alpha)}{2^\alpha \phi(2^\alpha)(2^\alpha, 4B)}.$$

To compute $C(2)$ recall Lemma 3.6.2 (4),

$$c_1(2^\alpha) = (-2)^\alpha$$

We compute

$$1 + \sum_{\alpha \geq 1} \frac{\phi((2^\alpha, 4B))c_1(2^\alpha)}{2^\alpha \phi(2^\alpha)(2^\alpha, 4B)} = \frac{2}{3}$$

Using Lemma 3.6.2 the following two computations allow us to simplify the first and second products in (3.42). First we compute, for $q \nmid B$

$$\sum_{\alpha\geq 0}\frac{c_1(q^\alpha)}{q^\alpha\phi(q^\alpha)} = \begin{cases} 1+\sum_{\alpha,\ \text{even}}^{\alpha\geq 1}\frac{q^{\alpha-1}(q-3)}{q^\alpha q^{\alpha-1}(q-1)}+\sum_{\alpha,\ \text{odd}}^{\alpha\geq 1}\frac{q^{\alpha-1}(-1-\left(\frac{-1}{q}\right))}{q^\alpha q^{\alpha-1}(q-1)} & \text{if } q\nmid r \\ 1+\sum_{\alpha\geq 1}\frac{\left(\frac{-1}{q}\right)^\alpha(\phi(q^\alpha))}{q^\alpha q^{\alpha-1}(q-1)} & \text{if } q|r \end{cases}$$

$$= \begin{cases} 1+\frac{(q-3)}{(q-1)(q^2-1)}+\frac{q\left(-1-\left(\frac{-1}{q}\right)\right)}{(q-1)(q^2-1)} & \text{if } q\nmid r \\ \frac{q^2+\left(\frac{-1}{q}\right)q}{q^2-1} & \text{if } q|r. \end{cases}$$

$$= \begin{cases} 1-\frac{\left(\frac{-1}{q}\right)q+3}{(q-1)(q^2-1)} & \text{if } q\nmid r \\ \frac{q}{q-\left(\frac{-1}{q}\right)} & \text{if } q|r. \end{cases}$$

Second, we compute for $q \nmid B$, $q \nmid r$

$$\begin{aligned} &\sum_{\beta\geq 1}\frac{2}{q^\beta\phi(q^{2\beta})}\sum_{\alpha\geq 0}\frac{\phi((q^\alpha,q^{2\beta}))c_q(q^\alpha)}{q^\alpha\phi(q^\alpha)(q^\alpha,q^{2\beta})2^{\nu(q^\beta,q^\alpha)}} \\ &= \sum_{\beta\geq 1}\frac{2}{q^\beta\phi(q^{2\beta})}\left[1+\frac{1}{2}\sum_{\alpha\geq 1}\frac{c_q(q^\alpha)}{q^\alpha q^\alpha}\right] \\ &= \frac{2q}{q-1}\sum_{\beta\geq 1}\frac{1}{q^{3\beta}}\left[1+\frac{1}{q(q+1)}\right] \\ &= \frac{2(q^2+q+1)}{q^2-1}\sum_{\beta\geq 1}\frac{1}{q^{3\beta}} \\ &= \frac{2(q^2+q+1)}{(q^2-1)(q^3-1)} \\ &= \frac{2}{(q^2-1)(q-1)} \end{aligned}$$

For the third product in (3.42) note that $q|B$ and $q|r$. Since $(k,r)=1$, $q \nmid k = q^{\beta}$. Therefore using Lemma 3.6.2 with $\beta = 0$

$$\begin{aligned}
1+\sum_{\alpha\geq 1}\frac{\phi(q^{\min(\alpha,\mathrm{ord}_q(B))})c_1(q^\alpha)}{q^\alpha\phi(q^\alpha)q^{\min(\alpha,\mathrm{ord}_q(B))}} &= 1+\sum_{1\leq\alpha\leq\mathrm{ord}_q(B)}\frac{c_1(q^\alpha)}{q^{2\alpha}}+\sum_{\mathrm{ord}_q(B)<\alpha}\frac{c_1(q^\alpha)}{q^{2\alpha}} \\
&= 1+\sum_{1\leq\alpha\leq\mathrm{ord}_q(B)}\frac{\left(\frac{-1}{q}\right)^\alpha}{q^{2\alpha}}+\sum_{\mathrm{ord}_q(B)<\alpha}q^{\alpha-\mathrm{ord}_q(B)}\left(\frac{-1}{q}\right)^\alpha\frac{1}{q^{2\alpha}} \\
&= 1+\frac{\left(\frac{-1}{q}\right)-\left(\frac{-1}{q}\right)^{\mathrm{ord}_q(B)+1}q^{-2\mathrm{ord}_q(B)}}{q^2-\left(\frac{-1}{q}\right)}+\frac{\left(\frac{-1}{q}\right)^{\mathrm{ord}_q(B)+1}}{q^{2\mathrm{ord}_q(B)}(q-\left(\frac{-1}{q}\right))}
\end{aligned}$$

(3.42) may now be written as

$$\begin{aligned}
C_{r,A,B} = \frac{d_2(1)}{\phi(4B)}\cdot\frac{2}{3} & \\
&\cdot\prod_{\substack{q,\mathrm{odd}\\ q\nmid B\\ q|r}}\left(\frac{q}{q-\left(\frac{-1}{q}\right)}\right)\prod_{\substack{q,\mathrm{odd}\\ q\nmid B\\ q\nmid r}}\left(1-\frac{\left(\frac{-1}{q}\right)q+3}{(q-1)(q^2-1)}+\frac{2}{(q^2-1)(q-1)}\right) \\
&\cdot\prod_{\substack{q,\mathrm{odd}\\ q|B\\ q|r}}\left(1+\frac{\left(\frac{-1}{q}\right)-\left(\frac{-1}{q}\right)^{\mathrm{ord}_q(B)+1}q^{-2\mathrm{ord}_q(B)}}{q^2-\left(\frac{-1}{q}\right)}+\frac{\left(\frac{-1}{q}\right)^{\mathrm{ord}_q(B)+1}}{q^{2\mathrm{ord}_q(B)}(q-\left(\frac{-1}{q}\right))}\right) \qquad (3.43)\\
&\cdot\prod_{\substack{q,\mathrm{odd}\\ q|B\\ q\nmid r}}\Bigg(1+\sum_{\alpha\geq 1}\frac{c_1(q^\alpha)}{q^{2\alpha}} \\
&\quad+\frac{d_q(1)}{f_q}\sum_{\beta\geq 1}\frac{1}{q^{3\beta}}\left(1+\sum_{\alpha\geq 1}\frac{2^{\nu\left(\frac{(q^\beta,B^2)}{(q^\beta,B)},q^\alpha\right)}c_{q^\beta}(q^\alpha)}{q^{2\alpha}2^{\nu\left(\frac{q^\beta}{(q^\beta,B)},q^\alpha\right)}}\right)\Bigg)
\end{aligned}$$

For the computation of the last product we use the following notation.

$$\Delta = r^2-4A^2 \qquad \Delta_q = \mathrm{ord}_q(\Delta) \qquad L_q = \left(\frac{r^2-4A^2}{q}\right)$$

Using Lemma 3.6.2 for the value of $c_1(q^\alpha)$ we have,

$$\begin{aligned}
&1+\sum_{\alpha\geq 1}\frac{c_1(q^\alpha)}{q^{2\alpha}}\\
&=1+\sum_{1\leq\alpha\leq \mathrm{ord}_q(B)}\frac{c_1(q^\alpha)}{q^{2\alpha}}+\sum_{\mathrm{ord}_q(B)+1\leq\alpha}\frac{c_1(q^\alpha)}{q^{2\alpha}}\\
&=1+\sum_{1\leq\alpha\leq \mathrm{ord}_q(B)}\frac{1}{q^{2\alpha}}L_q^\alpha+\sum_{\mathrm{ord}_q(B)+1\leq\alpha}\frac{L_q^\alpha}{q^{\alpha+\mathrm{ord}_q(B)}}\\
&=\begin{cases}1+\frac{L_q q^{2\mathrm{ord}_q(B)}-L_q^{\mathrm{ord}_q(B)+1}}{q^{2\mathrm{ord}_q(B)+2}-L_q q^{2\mathrm{ord}_q(B)}}+\frac{L_q^{\mathrm{ord}_q(B)+1}}{q^{2\mathrm{ord}_q(B)}(q-L_q)} & \text{if } \Delta_q=0\\ 1 & \text{if } \Delta_q>0.\end{cases}
\end{aligned}$$

We now deal with the remaining double sum in the fourth product. We first write the double sum as

$$\frac{d_q(1)}{f_q}\sum_{\beta\geq 1}\frac{1}{q^{3\beta}}\left(1+\sum_{\alpha\geq 1}\frac{2^{\nu\left(\frac{(q^\beta,B^2)}{(q^\beta,B)},q^\alpha\right)}c_{q^\beta}(q^\alpha)}{q^{2\alpha}2^{\nu\left(\frac{q^\beta}{(q^\beta,B)},q^\alpha\right)}}\right)=\frac{d_q(1)}{f_q}\sum_{\beta\geq 1}\frac{1}{q^{3\beta}}\left(1+\sum_{\alpha\geq 1}\frac{c_{q^\beta}(q^\alpha)}{q^{2\alpha}}\right)$$

Now we split the sum on $\beta\geq 1$ according to Lemma 3.6.2 (2) and simplify. Then the double sum becomes

$$\begin{aligned}
&\frac{d_q(1)}{f_q}\sum_{\beta\geq 1}\frac{\phi((B,q^{2\beta}))}{q^\beta\phi(q^{2\beta})(B,q^{2\beta})}\sum_{\alpha\geq 0}\frac{\phi((q^\alpha,Bq^{2\beta}))c_{q^\beta}(q^\alpha)}{q^\alpha\phi(q^\alpha)(q^\alpha,4Bq^{2\beta})}\\
&=\frac{d_q(1)}{f_q}\sum_{1<2\beta<\min(\mathrm{ord}_q(B),\Delta_q)}\frac{1}{q^{3\beta}}\left[1+\sum_{\alpha\geq 1}\frac{c_{q^\beta}(q^\alpha)}{q^{2\alpha}}\right]\\
&+\frac{d_q(1)}{f_q}\sum_{2\beta\geq\min(\mathrm{ord}_q(B),\Delta_q)}\frac{1}{q^{3\beta}}\left[1+\sum_{\alpha\geq 1}\frac{c_{q^\beta}(q^\alpha)}{q^{2\alpha}}\right] \qquad (3.44)
\end{aligned}$$

To evaluate this double sum we first make the following two observations

1. By the definition of f_q,

$$\frac{d_q(1)}{f_q}=\begin{cases}0 & \text{if } d_q(1)=0\\ 1 & \text{if } d_q(1)\neq 0.\end{cases}$$

2. Let $\mathrm{ord}_q(k)=\beta$. Note that since

$$d_q(1)=0\iff (B,q^{2\beta})\nmid\Delta$$

we have

$$\frac{d_q(1)}{f_q} = 0 \Longleftrightarrow \min(\mathrm{ord}_q(B), 2\beta) > \Delta_q.$$

Therefore, we examine three cases. Note that $\beta \geq 1$ and $\mathrm{ord}_q(B) \geq 1$.

Case 1: $\Delta_q = 0$

In this case $\frac{d_q(1)}{f_q} = 0$. Therefore the last product in (3.43) is

$$\prod_{\substack{q,\mathrm{odd}\\ q|B\\ q\nmid r}} \left(1 + \frac{L_q q^{2\mathrm{ord}_q(B)} - L_q^{\mathrm{ord}_q(B)+1}}{q^{2\mathrm{ord}_q(B)+2} - L_q q^{2\mathrm{ord}_q(B)}} + \frac{L_q^{\mathrm{ord}_q(B)+1}}{q^{2\mathrm{ord}_q(B)}(q - L_q)}\right).$$

Case 2: $1 \leq \mathrm{ord}_q(B) \leq \Delta_q$

In this case $\frac{d_q(1)}{f_q} = 1$. Since $c_{q^\beta}(q^\alpha) = 0$ whenever $2\beta < \Delta_q$, (3.44) becomes

$$\sum_{1<2\beta<\min(\mathrm{ord}_q(B),\Delta_q)=\mathrm{ord}_q(B)} \frac{1}{q^{3\beta}}\left[1+0\right] + \sum_{2\beta\geq\min(\mathrm{ord}_q(B),\Delta_q)=\mathrm{ord}_q(B)} \frac{1}{q^{3\beta}}\left[1 + \sum_{\alpha\geq 1}\frac{c_{q^\beta}(q^\alpha)}{q^{2\alpha}}\right].$$

The first sum is

$$\sum_{1<2\beta<\min(\mathrm{ord}_q(B),\Delta_q)=\mathrm{ord}_q(B)} \frac{1}{q^{3\beta}} = \frac{1 - q^{-3\left\lceil\frac{\mathrm{ord}_q(B)}{2}-1\right\rceil}}{q^3-1}.$$

Using Lemma 3.6.2 (2a) to obtain $c_{q^\beta}(q^\alpha)$ for $2\beta \geq \mathrm{ord}_q(B)$ the second sum is

$$\begin{aligned}
&\sum_{2\beta\geq\mathrm{ord}_q(B)} \frac{1}{q^{3\beta}}\left[1 + \sum_{\substack{\alpha\geq 1\\ \alpha\ \mathrm{even}}}\frac{q^{\mathrm{ord}_q(B)}\phi(q^\alpha)}{q^{2\alpha}}\right]\\
&= \sum_{2\beta\geq\mathrm{ord}_q(B)} \frac{1}{q^{3\beta}}\left[1 + \sum_{\substack{\alpha\geq 1\\ \alpha\ \mathrm{even}}}\frac{q-1}{q^{\alpha+1}}q^{\mathrm{ord}_q(B)}\right]\\
&= \sum_{2\beta\geq\mathrm{ord}_q(B)} \frac{1}{q^{3\beta}}\left[1 + \frac{q^{\mathrm{ord}_q(B)}}{q(q+1)}\right]\\
&= \left(\frac{q(q+1)+q^{\mathrm{ord}_q(B)}}{q(q+1)}\right)\sum_{2\beta\geq\mathrm{ord}_q(B)}\frac{1}{q^{3\beta}}\\
&= \frac{(q^2+q+q^{\mathrm{ord}_q(B)})q^{2-2\left\lceil\frac{\mathrm{ord}_q(B)}{2}\right\rceil}}{(q+1)(q^3-1)}
\end{aligned}$$

Therefore, in the case that $1 \le \mathrm{ord}_q(B) \le \Delta_q$ we may write the last product in (3.43) as

$$\prod_{\substack{q,\text{odd}\\ q|B\\ q\nmid r}} \left(1 + \frac{1 - q^{-3\left\lceil \frac{\mathrm{ord}_q(B)}{2} - 1\right\rceil}}{q^3 - 1} + \frac{(q^2 + q + q^{\mathrm{ord}_q(B)})q^{2-2\left\lceil \frac{\mathrm{ord}_q(B)}{2}\right\rceil}}{(q+1)(q^3-1)}\right)$$

Case 3: $\mathrm{ord}_q(B) > \Delta_q > 0$

We examine carefully the two sums in (3.44). In order to determine $\frac{d_q(1)}{f_q}$, we examine $\min(\mathrm{ord}_q(B), 2\beta)$ by using observation 2 on page 129.

1. In the first sum we sum over $1 < 2\beta < \min(\mathrm{ord}_q(B), \Delta_q) = \Delta_q$.

$$\frac{d_q(1)}{f_q} = \begin{cases} 1 & \text{if } \min(\mathrm{ord}_q(B), 2\beta) = 2\beta \\ 0 & \text{if } \min(\mathrm{ord}_q(B), 2\beta) = \mathrm{ord}_q(B). \end{cases}$$

   By Lemma 3.6.2 2(b), $c_{q^\beta}(q^\alpha) = 0$, since $\Delta_q > 2\beta$. Therefore, the first sum becomes

$$\begin{aligned} &\frac{d_q(1)}{f_q} \sum_{1<2\beta<\min(\mathrm{ord}_q(B),\Delta_q)=\Delta_q} \frac{1}{q^{3\beta}} [1+0] \\ &= \sum_{1<2\beta<\min(\mathrm{ord}_q(B),\Delta_q)=\Delta_q} \frac{1}{q^{3\beta}} \end{aligned}$$

2. In the second sum we sum over $2\beta \ge \min(\mathrm{ord}_q(B), \Delta_q) = \Delta_q$. If $\min(\mathrm{ord}_q(B), 2\beta) = \mathrm{ord}_q(B)$, then $d_q(1)/f_q = 0$. If $\min(\mathrm{ord}_q(B), 2\beta) = 2\beta$, then $d_q(1)/f_q = 1$ if and only if $2\beta = \Delta_q$, since $2\beta \ge \Delta_q$ For the second sum we also include the sum on $\alpha \ge 1$, since if $2\beta = \Delta_q$, then $c_{q^\beta}(q^\alpha) \ne 0$, by Lemma 3.6.2 2(b). Therefore, the second sum becomes

$$\begin{aligned} &\frac{d_q(1)}{f_q} \sum_{2\beta\ge\min(\mathrm{ord}_q(B),\Delta_q)=\Delta_q} \frac{1}{q^{3\beta}} \left[1 + \sum_{\alpha\ge1} \frac{c_{q^\beta}(q^\alpha)}{q^{2\alpha}}\right] \\ &= \frac{d_q(1)}{f_q} \sum_{\beta=\left\lceil\frac{\Delta_q}{2}\right\rceil}^{\infty} \frac{1}{q^{3\beta}} \left[1 + \sum_{\alpha\ge1} \frac{c_{q^\beta}(q^\alpha)}{q^{2\alpha}}\right] \\ &= \begin{cases} \frac{1}{q^{3\Delta_q/2}} \left[1 + \sum_{\alpha\ge1} \frac{q^{\alpha-\min(\alpha,\mathrm{ord}_q(B)-\Delta_q)\gamma_q^\alpha}}{q^{2\alpha}}\right] & \text{if } \Delta_q \equiv 0 \pmod 2 \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

where

$$\gamma_q = \left(\frac{\Delta / q^{\Delta_q}}{q} \right).$$

Therefore, (3.44) on page 129 becomes

$$\begin{aligned}
&\frac{d_q(1)}{f_q} \sum_{1<2\beta<\min(\mathrm{ord}_q(B),\Delta_q)} \frac{1}{q^{3\beta}} \left[1 + \sum_{\alpha \geq 1} \frac{c_{q^\beta}(q^\alpha)}{q^{2\alpha}} \right] \\
&\qquad + \frac{d_q(1)}{f_q} \sum_{2\beta \geq \min(\mathrm{ord}_q(B),\Delta_q)} \frac{1}{q^{3\beta}} \left[1 + \sum_{\alpha \geq 1} \frac{c_{q^\beta}(q^\alpha)}{q^{2\alpha}} \right] \\
&= \begin{cases} \sum_{1<2\beta<\min(\mathrm{ord}_q(B),\Delta_q)=\Delta_q} \frac{1}{q^{3\beta}} & \\ \quad + q^{-3\Delta_q/2} \left[1 + \sum_{\alpha \geq 1} q^{-\alpha - \min(\alpha, \mathrm{ord}_p(B) - \Delta_q)} \gamma_q^\alpha \right] & \text{if } \Delta_q \equiv 0 \pmod 2 \\ \sum_{1<2\beta<\min(\mathrm{ord}_q(B),\Delta_q)=\Delta_q} \frac{1}{q^{3\beta}} & \text{if } \Delta_q \equiv 1 \pmod 2. \end{cases}
\end{aligned}$$

Therefore, if $\Delta_q \equiv 0 \pmod 2$ the double sum (3.44) simplifies to

$$\frac{1 - q^{-3(\Delta_q/2-1)}}{q^3 - 1} + \frac{1}{q^{3\Delta_q/2}} \left[1 + \gamma_q \left[\frac{(q^{2(\mathrm{ord}_q(B)-\Delta_q)} - \gamma_q^{\mathrm{ord}_q(B)-\Delta_q})(q - \gamma_q) + \gamma_q^{\mathrm{ord}_q(B)-\Delta_q}(q^2 - \gamma_q)}{q^{2(\mathrm{ord}_q(B)-\Delta_q)}(q - \gamma_q)(q^2 - \gamma_q)} \right] \right].$$

If $\Delta_q \equiv 1 \pmod 2$ the double sum (3.44) simplifies to

$$\frac{1 - q^{-3\lceil \Delta_q/2 - 1 \rceil}}{q^3 - 1}.$$

We have shown that

$$C_{r,A,B} = \frac{2}{3\phi(B)} \prod_{\substack{q,\text{odd}\\ q\nmid B\\ q\mid r}} \left(\frac{q}{q - \left(\frac{-1}{q}\right)} \right) \prod_{\substack{q,\text{odd}\\ q\nmid B\\ q\nmid r}} \left(1 - \frac{\left(\frac{-1}{q}\right) q - 1}{(q-1)(q^2-1)} \right)$$

$$\cdot \prod_{\substack{q,\text{odd}\\ q\mid B\\ q\mid r}} \left(1 + \frac{\left(\frac{-1}{q}\right) - \left(\frac{-1}{q}\right)^{\text{ord}_q(B)+1} q^{-2\text{ord}_q(B)}}{q^2 - \left(\frac{-1}{q}\right)} + \frac{\left(\frac{-1}{q}\right)^{\text{ord}_q(B)+1}}{q^{2\text{ord}_q(B)}\left(q - \left(\frac{-1}{q}\right)\right)} \right)$$

$$\cdot \prod_{\substack{q,\text{odd}\\ q\mid B\\ q\nmid r\\ \Delta_q=0}} \left(1 + \frac{L_q q^{2\text{ord}_q(B)} - L_q^{\text{ord}_q(B)+1}}{q^{2\text{ord}_q(B)+2} - L_q q^{2\text{ord}_q(B)}} + \frac{L_q^{\text{ord}_q(B)+1}}{q - L_q} \right)$$

$$\cdot \prod_{\substack{q,\text{odd}\\ q\in\mathfrak{P}^{\leq}_{r,A,B}}} \left(1 + \frac{1 - q^{-3\left\lceil \frac{\text{ord}_q(B)}{2} - 1 \right\rceil}}{q^3 - 1} + \frac{(q^2 + q + q^{\text{ord}_q(B)}) q^{2-2\left\lceil \frac{\text{ord}_q(B)}{2} \right\rceil}}{(q+1)(q^3-1)} \right)$$

$$\cdot \prod_{\substack{q,\text{odd}\\ q\in\mathfrak{P}^{>}_{r,A,B}\\ \Delta_q\equiv 1 \pmod 2}} \left(\frac{1 - q^{-3\lceil \Delta_q/2 - 1 \rceil}}{q^3 - 1} \right)$$

$$\cdot \prod_{\substack{q,\text{odd}\\ q\in\mathfrak{P}^{>}_{r,A,B}\\ \Delta_q\equiv 0 \pmod 2}} \left(\frac{1 - q^{-3(\Delta_q/2-1)}}{q^3-1} + \right.$$

$$\left. \frac{1}{q^{3\Delta_q/2}} \left[1 + \gamma_q \left[\frac{(q^{2(\text{ord}_q(B)-\Delta_q)} - \gamma_q^{\text{ord}_q(B)-\Delta_q})(q-\gamma_q) + \gamma_q^{\text{ord}_q(B)-\Delta_q}(q^2-\gamma_q)}{q^{2(\text{ord}_q(B)-\Delta_q)}(q-\gamma_q)(q^2-\gamma_q)} \right] \right] \right)$$

where

$$\mathfrak{P}^{\leq}_{r,A,B} = \{q > 2, \text{prime} : q|B; q \nmid r; \text{ord}_q(B) \leq \Delta_q\} \quad \text{and}$$

$$\mathfrak{P}^{>}_{r,A,B} = \{q > 2, \text{prime} : q|B; q \nmid r; \text{ord}_q(B) > \Delta_q > 0\}.$$

This completes the proof of Lemma 3.0.21.

□

CHAPTER 4

Future Work

In chapter 2 we showed that the Selmer groups S_n and S'_n of the congruent number curve are related to certain graphs. Using graph theoretic methods we computed the size of these groups using only linear algebra. Silverman's proposition (see pg. 15) applies to curves which have a point of order two. Therefore, if one defines the proper graphs then the techniques of chapter 2 can be used to find the size of the Selmer groups for any elliptic curve with at least one rational point of order two.

Using results found in [6] along with cubic residue characters it may be possible to give a graphical interpretation of 3-Selmer groups (see [11, §3]).

In [21] Hurrelbrink gives results on certain graphs that yield information about the structure of the ideal class group of some quadratic number fields. These graphs are constructed in a similar fashion as our graphs in chapter 2. In particular, vertices represent primes congruent to 1 modulo 4 and two vertices are adjacent whenever their legendre symbol is -1. Moreover, Hurrelbrink defines an Eulerian Vertex Decomposition of a graph which turns out to be an even partition as defined on page 22. This suggests there may be a connection between Selmer groups and class groups which may be explored using graph theoretic concepts.

In chapter 3 we proved an average result for a general version of the Lang-Trotter conjecture (see pg. 18). Our techniques worked for Abelian extensions because of Corollary 3.0.16. Unfortunately these techniques do not work for any extensions of $\mathbb{Q}$. It may be possible to obtain an average result of the conjecture over any Galois extensions by using Chebotarev's density theorem.

INDEX

BIBLIOGRAPHY

1. Amir Akbary, Chantal David, and Robert Juricevic. Average distributions and products of special values of L-series. *Acta Arith.*, 111(3):239–268, 2004.

2. S. Baier. The Lang-Trotter conjecture on average. *To appear.*

3. Jonathan Battista, Jonathan Bayless, Dmitriy Ivanov, and Kevin James. Average Frobenius distributions for elliptic curves with nontrivial rational torsion. *Acta Arith.*, 119(1):81–91, 2005.

4. Morgan V. Brown, Neil J. Calkin, Kevin James, Adam J. King, Shannon Lockard, and Robert C. Rhoades. Trivial Selmer groups and even partitions of a graph. *Integers*, 6:A33, 17 pp. (electronic), 2006.

5. J. W. S. Cassels. Diophantine equations with special reference to elliptic curves. *J. London Math. Soc.*, 41:193–291, 1966.

6. Yen-Mei Julia Chen. *Descent via 3-isogenies on elliptic curves.* PhD thesis, Brown University, 1993.

7. Chantal David and Francesco Pappalardi. Average Frobenius distributions of elliptic curves. *Internat. Math. Res. Notices*, (4):165–183, 1999.

8. Chantal David and Francesco Pappalardi. Average Frobenius distribution for inerts in $\mathbb{Q}(i)$. *J. Ramanujan Math. Soc.*, 19(3):181–201, 2004.

9. Max Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hansischen Univ.*, 14:197–272, 1941.

10. Darrin Doud. A procedure to calculate torsion of elliptic curves over $\mathbf{Q}$. *Manuscripta Math.*, 95(4):463–469, 1998.

11. Noam D. Elkies and Nicholas F. Rogers. Elliptic curves $x^3 + y^3 = k$ of high rank. In *Algorithmic number theory*, volume 3076 of *Lecture Notes in Comput. Sci.*, pages 184–193. Springer, Berlin, 2004.

12. Bryan Faulkner and Kevin James. A graphical approach to computing Selmer groups of congruent number curves. *Ramanujan J.*, 14(1):107–129, 2007.

13. Keqin Feng and Maosheng Xiong. On elliptic curves $y^2 = x^3 - n^2x$ with rank zero. *J. Number Theory*, 109(1):1–26, 2004.

14. É. Fouvry and M. Ram Murty. Supersingular primes common to two elliptic curves. In *Number theory (Paris, 1992–1993)*, volume 215 of *London Math. Soc. Lecture Note Ser.*, pages 91–102. Cambridge Univ. Press, Cambridge, 1995.

15. Etienne Fouvry and M. Ram Murty. On the distribution of supersingular primes. *Canad. J. Math.*, 48(1):81–104, 1996.

16. Takeshi Goto. *A study on the Selmer groups of elliptic curves with a rational 2-torsion*. PhD thesis, Kyushu University, 2002.

17. G. H. Hardy and J. E. Littlewood. Some problems of 'Partitio numerorum' (VI): Further researches in Waring's Problem. *Math. Z.*, 23(1):1–37, 1925.

18. G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers*. The Clarendon Press Oxford University Press, New York, fifth edition, 1979.

19. D. R. Heath-Brown. The size of Selmer groups for the congruent number problem. *Invent. Math.*, 111(1):171–195, 1993.

20. D. R. Heath-Brown. The size of Selmer groups for the congruent number problem. II. *Invent. Math.*, 118(2):331–370, 1994.

21. Jürgen Hurrelbrink. Circulant graphs and 4-ranks of ideal class groups. *Canad. J. Math.*, 46(1):169–183, 1994.

22. Kevin James. Average Frobenius distributions for elliptic curves with 3-torsion. *J. Number Theory*, 109(2):278–298, 2004.

23. Kevin James. Averaging special values of Dirichlet L-series. *Ramanujan J.*, 10(1):75–87, 2005.

24. Kevin James and Ken Ono. Selmer groups of quadratic twists of elliptic curves. *Math. Ann.*, 314(1):1–17, 1999.

25. Robert Juricevic. Average Lang-Trotter conjecture for 2 elliptic curves. Master's thesis, Concordia University, 2000.

26. Serge Lang and Hale Trotter. *Frobenius distributions in* GL_2*-extensions*. Springer-Verlag, Berlin, 1976. Distribution of Frobenius automorphisms in GL_2-extensions of the rational numbers, Lecture Notes in Mathematics, Vol. 504.

27. H. W. Lenstra, Jr. Factoring integers with elliptic curves. *Ann. of Math. (2)*, 126(3):649–673, 1987.

28. L.J. Mordell. On the rational solutions of the indeterminate equations of the third and fourth degrees. *Proc. London Math. Soc.*, 21:179–182, 1922.

29. M. Ram Murty. *Problems in analytic number theory*, volume 206 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2001. , Readings in Mathematics.

30. René Schoof. Nonsingular plane cubic curves over finite fields. *J. Combin. Theory Ser. A*, 46(2):183–211, 1987.

31. Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

32. Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

33. Joseph H. Silverman and John Tate. *Rational points on elliptic curves*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992.

34. Gérald Tenenbaum. *Introduction to analytic and probabilistic number theory*, volume 46 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1995. Translated from the second French edition (1995) by C. B. Thomas.

35. Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.

36. A. Weil. L'arithmetique sur les courbes algébriques. *Acta Math.*, 52:281–315, 1928.

37. Gang Yu. Average size of 2-Selmer groups of elliptic curves. II. *Acta Arith.*, 117(1):1–33, 2005.